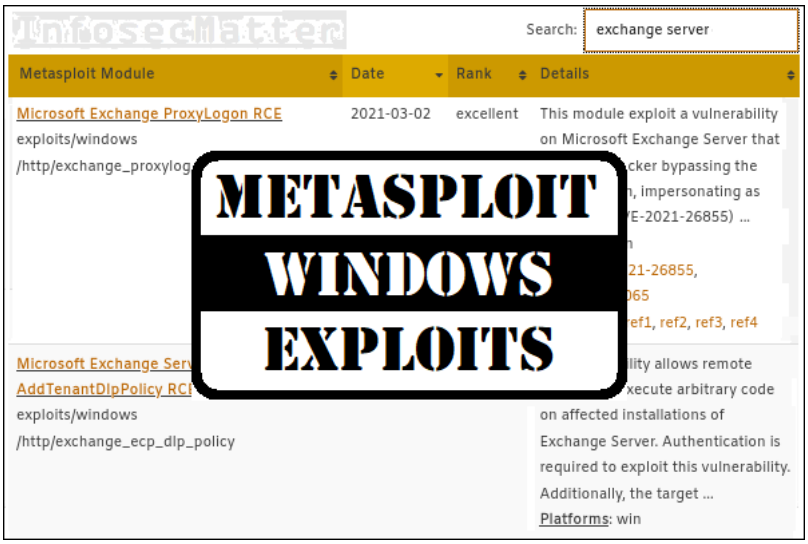
List of Metasploit Windows Exploits (Detailed Spreadsheet)

infosecmatter.com/list-of-metasploit-windows-exploits-detailed-spreadsheet

April 15, 2021



On this page you will find a comprehensive list of all **Metasploit Windows exploits** that are currently available in the open source version of the Metasploit Framework, the number one penetration testing platform.

It is my hope that this list will help you navigate through the vast lists of Metasploit exploits more easily and help you to save time during your penetration testing engagements.

Introduction

There are currently over 2,120 exploit modules in the latest Metasploit Framework release. The list below contains 1,325 of them which are either:

- Directly targeted for Windows systems (`exploit/windows/...`) or
- Affecting Windows systems as well (e.g. `exploit/multi/...`)

Thus, this list should contain all Metasploit exploits that can be used against Windows based systems.

The list is organized in an interactive table (spreadsheet) with the most important information about each module in one row, namely:

- Exploit module name with a brief description of the exploit
- List of platforms and CVEs (if specified in the module)
- Reference links in the module providing more details

The spreadsheet is interactive and it allows to:

- Use the search filtering to quickly find relevant exploits (see examples below)
- See the detailed module library entry by clicking on the module name
- Sort the columns (in ascending or descending order)

Filtering examples

As mentioned above, you can use the search function to interactively filter out the exploits based on a pattern of your interest. Here are couple of examples:

- Search for: **`sharepoint rce`**
  Display only remote code execution exploits for Microsoft SharePoint.
- Search for: **`cve-2020`**
  Display only exploits with assigned CVE from year 2020.
- Search for **`eternalblue`**
  Display only modules for exploiting the MS17-010 SMB vulnerability.
- Search for **`privilege escalation`**
  Display only Windows privilege escalation exploits.
- Search for: **`bypassuac`**
  Display only bypass UAC exploits.
- Search for: **`proxylogon`**
  Display only modules exploiting vulnerabilities against Microsoft Exchange Server.

Alright, now let's get to the list.

List of Metasploit Windows exploits

Metasploit Module	Date	Rank	Details
Firefox Exec Shellcode from Privileged Javascript Shell exploit/firefox/local/exec_shellcode	2014-03-10	excellent	This module allows execution of native pay from a privileged Firefox Javascript shell. It places the specified payload into memory, the necessary protection flags, and calls it, which can ... **Platforms**: firefox, linux, osx, unix, win **Refs**: source
Firefox PDF.js Privileged Javascript Injection exploit/multi/browser/firefox_pdfjs_privilege_escalation	2015-03-31	manual	This module gains remote code execution Firefox 35-36 by abusing a privilege escala bug in resource:// URIs. PDF.js is used to e the bug. This exploit requires the user to cl anywhere ... **Platforms**: firefox, java, linux, osx, solaris, **CVEs**: CVE-2015-0802, CVE-2015-0816 **Refs**: source
Java Applet JAX-WS Remote Code Execution exploit/multi/browser/java_jre17_jaxws	2012-10-16	excellent	This module abuses the JAX-WS classes f Java Applet to run arbitrary Java code outs of the sandbox as exploited in the wild in November of 2012. The vulnerability affect Java version 7u7 and ... **Platforms**: java, linux, win **CVEs**: CVE-2012-5067, CVE-2012-5076 **Refs**: source, ref1, ref2, ref3
Adobe Flash Player ByteArray Use After Free exploit/multi/browser/adobe_flash_hacking_team_uaf	2015-07-06	great	This module exploits an use after free on A Flash Player. The vulnerability, discovered Hacking Team and made public as part of t July 2015 data leak, was described as an U After Free ... **Platforms**: linux, win **CVEs**: CVE-2015-5119 **Refs**: source, ref1, ref2, ref3
Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow exploit/multi/browser/adobe_flash_nellymoser_bof	2015-06-23	great	This module exploits a buffer overflow on A Flash Player when handling nellymoser encoded audio inside a FLV video, as expl in the wild on June 2015. This module has tested successfully ... **Platforms**: linux, win **CVEs**: CVE-2015-3043, CVE-2015-3113 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Adobe Flash Player NetConnection Type Confusion exploit/multi/browser/adobe_flash_net_connection_confusion	2015-03-12	great	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 ... **Platforms**: linux, win **CVEs**: CVE-2015-0336 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Adobe Flash opaqueBackground Use After Free exploit/multi/browser/adobe_flash_opaque_background_uaf	2015-07-06	great	This module exploits an use after free on A Flash Player. The vulnerability, discovered Hacking Team and made public as part of t July 2015 data leak, was described as an U After Free ... **Platforms**: win **CVEs**: CVE-2015-5122 **Refs**: source, ref1, ref2, ref3
Adobe Flash Player Shader Buffer Overflow exploit/multi/browser/adobe_flash_pixel_bender_bof	2014-04-28	great	This module exploits a buffer overflow vulnerability in Adobe Flash Player. The vulnerability occurs in the flash.Display.Sha class, when setting specially crafted data a bytecode, as ... **Platforms**: linux, win **CVEs**: CVE-2014-0515 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Adobe Flash Player Drawing Fill Shader Memory Corruption exploit/multi/browser/adobe_flash_shader_drawing_fill	2015-05-12	great	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 succes on: Windows 7 SP1 (32-bit), ... **Platforms**: linux, win **CVEs**: CVE-2015-3105 **Refs**: source, ref1, ref2, ref3, ref4
Adobe Flash Player ShaderJob Buffer Overflow exploit/multi/browser/adobe_flash_shader_job_overflow	2015-05-12	great	This module exploits a buffer overflow vulnerability related to the ShaderJob work on Adobe Flash Player. The vulnerability happens when trying to apply a Shader set up the same Bitmap object ... **Platforms**: linux, win **CVEs**: CVE-2015-3090 **Refs**: source, ref1, ref2, ref3, ref4
Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free exploit/multi/browser/adobe_flash_uncompress_zlib_uaf	2014-04-28	great	This module exploits a use after free vulnerability in Adobe Flash Player. The vulnerability occurs in the ByteArray::UncompressViaZlibVariant meth when trying to uncompress() a malformed ... **Platforms**: linux, win **CVEs**: CVE-2015-0311 **Refs**: source, ref1, ref2, ref3
Google Chrome 72 and 73 Array.map exploit exploit/multi/browser/chrome_array_map	2019-03-07	manual	This module exploits an issue in Chrome 73.0.3683.86 (64 bit). The exploit corrupts length of a float in order to modify the back store of a typed array. The typed array can be used to ... **Platforms**: osx, win **CVEs**: CVE-2019-5825 **Refs**: source, ref1, ref2, ref3, ref4
Google Chrome 80 JSCreate side-effect type confusion exploit exploit/multi/browser/chrome_jscreate_sideeffect	2020-02-19	manual	This module exploits an issue in Google Chrome 80.0.3987.87 (64 bit). The exploit corrupts the length of a float array (float_re which can then be used for out of bounds r and write on adjacent ... **Platforms**: osx, win **CVEs**: CVE-2020-6418 **Refs**: source, ref1, ref2, ref3
Google Chrome 67, 68 and 69 Object.create exploit exploit/multi/browser/chrome_object_create	2018-09-25	manual	This modules exploits a type confusion in Google Chromes JIT compiler. The Object.create operation can be used to cau type confusion between a PropertyArray ar NameDictionary. The payload is ... **Platforms**: linux, osx, win **CVEs**: CVE-2018-17463, CVE-2019-1458 **Refs**: source, ref1, ref2, ref3, ref4
Google Chrome versions before 87.0.4280.88 integer overflow during SimplfiedLowering phase exploit/multi/browser/chrome_simplifiedlowering_overflow	2020-11-19	manual	This module exploits an issue in Google Chrome versions before 87.0.4280.88 (64 The exploit makes use of a integer overflo the SimplifiedLowering phase in turbofan. I used along with a ... **Platforms**: linux, osx, win **CVEs**: CVE-2020-16040 **Refs**: source, ref1, ref2, ref3, ref4
Firefox 3.5 escape() Return Value Memory Corruption exploit/multi/browser/firefox_escape_retval	2009-07-13	normal	This module exploits a memory corruption vulnerability in the Mozilla Firefox browser. flaw occurs when a bug in the javascript interpreter fails to preserve the return value the escape() ... **Platforms**: osx, win **CVEs**: CVE-2009-2477 **Refs**: source, ref1
Firefox Proxy Prototype Privileged Javascript Injection exploit/multi/browser/firefox_proxy_prototype	2014-01-20	manual	This exploit gains remote code execution o Firefox 31-34 by abusing a bug in the XPConnect component and gaining a refer to the privileged chrome:// window. This ex requires the user to ... **Platforms**: firefox, java, linux, osx, solaris, **CVEs**: CVE-2014-8636, CVE-2015-0802 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Firefox 17.0.1 Flash Privileged Code Injection exploit/multi/browser/firefox_svg_plugin	2013-01-08	excellent	This exploit gains remote code execution o Firefox 17 and 17.0.1, provided the user ha installed Flash. No memory corruption is us First, a Flash object is cloned into the anonymous content of ... **Platforms**: firefox, java, linux, osx, solaris, **CVEs**: CVE-2013-0757, CVE-2013-0758 **Refs**: source, ref1, ref2
Firefox toString console.time Privileged Javascript Injection exploit/multi/browser/firefox_tostring_console_injection	2013-05-14	excellent	This exploit gains remote code execution o Firefox 15-22 by abusing two separate Javascript-related vulnerabilities to ultimate inject malicious Javascript code into a cont running with ... **Platforms**: firefox, java, linux, osx, solaris, **CVEs**: CVE-2013-1670, CVE-2013-1710 **Refs**: source
Firefox WebIDL Privileged Javascript Injection exploit/multi/browser/firefox_webidl_injection	2014-03-17	excellent	This exploit gains remote code execution o Firefox 22-27 by abusing two separate priv escalation vulnerabilities in Firefox's Javas APIs. **Platforms**: firefox, java, linux, osx, solaris, **CVEs**: CVE-2014-1510, CVE-2014-1511 **Refs**: source
Java AtomicReferenceArray Type Violation Vulnerability exploit/multi/browser/java_atomicreferencearray	2012-02-14	excellent	This module exploits a vulnerability due to fact that AtomicReferenceArray uses the U class to store a reference in an array direct which may violate type safety if not used properly. ... **Platforms**: java, linux, osx, solaris, win **CVEs**: CVE-2012-0507 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Sun Java Calendar Deserialization Privilege Escalation exploit/multi/browser/java_calendar_deserialize	2008-12-03	excellent	This module exploits a flaw in the deserializ of Calendar objects in the Sun JVM. The payload can be either a native payload whi generated as an executable and dropped/executed on the ... **Platforms**: java, linux, osx, solaris, win **CVEs**: CVE-2008-5353 **Refs**: source, ref1, ref2, ref3
Sun Java JRE getSoundbank file:// URI Buffer Overflow exploit/multi/browser/java_getsoundbank_bof	2009-11-04	great	This module exploits a flaw in the getSoundbank function in the Sun JVM. Th payload is serialized and passed to the app via PARAM tags. It must be a native payloa The effected Java versions are ... **Platforms**: linux, osx, win **CVEs**: CVE-2009-3867 **Refs**: source
Java Applet Driver Manager Privileged toString() Remote Code Execution exploit/multi/browser/java_jre17_driver_manager	2013-01-10	excellent	This module abuses the java.sql.DriverMar class where the toString() method is called user supplied classes from a doPrivileged The vulnerability affects Java version 7u17 ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-1488 **Refs**: source, ref1, ref2
Java 7 Applet Remote Code Execution exploit/multi/browser/java_jre17_exec	2012-08-26	excellent	The exploit takes advantage of two issues JDK 7: The ClassFinder and MethodFinder.findMethod(). Both were nev introduced in JDK 7. ClassFinder is a replacement for classForName back in JDI ... **Platforms**: java, linux, win **CVEs**: CVE-2012-4681 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7
Java Applet AverageRangeStatisticImpl Remote Code Execution exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl	2012-10-16	excellent	This module abuses the AverageRangeStatisticImpl from a Java Ap to run arbitrary Java code outside of the sandbox, a different exploit vector than the exploited in the wild in November of ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2012-5076 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Java Applet JMX Remote Code Execution exploit/multi/browser/java_jre17_jmxbean	2013-01-10	excellent	This module abuses the JMX classes from Java Applet to run arbitrary Java code outs of the sandbox as exploited in the wild in January of 2013. The vulnerability affects J version 7u10 and ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-0422 **Refs**: source, ref1, ref2, ref3
Java Applet JMX Remote Code Execution exploit/multi/browser/java_jre17_jmxbean_2	2013-01-19	excellent	This module abuses the JMX classes from Java Applet to run arbitrary Java code outs of the sandbox as exploited in the wild in February of 2013. Additionally, this module bypasses default ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-0431 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Java Applet Method Handle Remote Code Execution exploit/multi/browser/java_jre17_method_handle	2012-10-16	excellent	This module abuses the Method Handle cl from a Java Applet to run arbitrary Java co outside of the sandbox. The vulnerability a Java version 7u7 and earlier. **Platforms**: java, linux, osx, win **CVEs**: CVE-2012-5088 **Refs**: source, ref1, ref2
Java Applet ProviderSkeleton Insecure Invoke Method exploit/multi/browser/java_jre17_provider_skeleton	2013-06-18	great	This module abuses the insecure invoke() method of the ProviderSkeleton class that allows to call arbitrary static methods with supplied arguments. The vulnerability affec Java version 7u21 ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-2460 **Refs**: source, ref1, ref2, ref3, ref4
Java Applet Reflection Type Confusion Remote Code Execution exploit/multi/browser/java_jre17_reflection_types	2013-01-10	excellent	This module abuses Java Reflection to ger a Type Confusion, due to a weak access c when setting final fields on static classes, a run code outside of the Java Sandbox. The vulnerability ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-2423 **Refs**: source, ref1, ref2, ref3, ref4
Java Applet Rhino Script Engine Remote Code Execution exploit/multi/browser/java_rhino	2011-10-18	excellent	This module exploits a vulnerability in the R Script Engine that can be used by a Java A to run arbitrary Java code outside of the sandbox. The vulnerability affects version version 6 ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2011-3544 **Refs**: source, ref1
Sun Java JRE AWT setDiffICM Buffer Overflow exploit/multi/browser/java_setdifficm_bof	2009-11-04	great	This module exploits a flaw in the setDiffIC function in the Sun JVM. The payload is serialized and passed to the applet via PAR tags. It must be a native payload. The effec Java versions are ... **Platforms**: linux, osx, win **CVEs**: CVE-2009-3869 **Refs**: source
Java Signed Applet Social Engineering Code Execution exploit/multi/browser/java_signed_applet	1997-02-19	excellent	This exploit dynamically creates a .jar file v Msf::Exploit::Java mixin, then signs the it. T resulting signed applet is presented to the via a web page with an applet tag. The ... **Platforms**: java, linux, osx, solaris, win **Refs**: source, ref1
Java storeImageArray() Invalid Array Indexing Vulnerability exploit/multi/browser/java_storeimagearray	2013-08-12	great	This module abuses an Invalid Array Index Vulnerability on the static function storeImageArray() function in order to caus memory corruption and escape the Java Sandbox. The vulnerability ... **Platforms**: java, linux, win **CVEs**: CVE-2013-2465 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Java Statement.invoke() Trusted Method Chain Privilege Escalation exploit/multi/browser/java_trusted_chain	2010-03-31	excellent	This module exploits a vulnerability in Java Runtime Environment that allows an untrus method to run in a privileged context. The vulnerability affects version 6 prior to updat and version 5 ... **Platforms**: java, linux, win **CVEs**: CVE-2010-0840 **Refs**: source, ref1
Java Applet Field Bytecode Verifier Cache Remote Code Execution exploit/multi/browser/java_verifier_field_access	2012-06-06	excellent	This module exploits a vulnerability in HotS bytecode verifier where an invalid optimiza of GETFIELD/PUTFIELD/GETSTATIC/PUTS instructions leads to insufficient type check This allows a ... **Platforms**: java, linux, osx, solaris, win **CVEs**: CVE-2012-1723 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Mozilla Suite/Firefox compareTo() Code Execution exploit/multi/browser/mozilla_compareto	2005-07-13	normal	This module exploits a code execution vulnerability in the Mozilla Suite, Mozilla Fi and Mozilla Thunderbird applications. This exploit module is a direct port of Aviv Raff's HTML PoC. **Platforms**: win **CVEs**: CVE-2005-2265 **Refs**: source, ref1
Mozilla Suite/Firefox Navigator Object Code Execution exploit/multi/browser/mozilla_navigatorjava	2006-07-25	normal	This module exploits a code execution vulnerability in the Mozilla Suite, Mozilla Fi and Mozilla Thunderbird applications. This exploit requires the Java plugin to be instal **Platforms**: linux, osx, win **CVEs**: CVE-2006-3677 **Refs**: source, ref1
Metasploit msfd Remote Code Execution via Browser exploit/multi/browser/msfd_rce_browser	2018-04-11	normal	Metasploit's msfd-service makes it possible get a msfconsole-like interface over a TCP socket. This module connects to the msfd-socket through the victim's browser. To exe msfconsole-commands ... **Platforms**: ruby **Refs**: source
Opera 9 Configuration Overwrite exploit/multi/browser/opera_configoverwrite	2007-03-05	excellent	Opera web browser in versions <= 9.10 all unrestricted script access to its configuratio page, opera:config, allowing an attacker to change settings and potentially execute arbitrary code. **Platforms**: unix, win **Refs**: source
Opera historysearch XSS exploit/multi/browser/opera_historysearch	2008-10-23	excellent	Certain constructs are not escaped correct Opera's History Search results. These can used to inject scripts into the page, which c then be used to modify configuration settin and execute ... **Platforms**: unix, win **CVEs**: CVE-2008-4696 **Refs**: source, ref1
Apple QTJava toQTPointer() Arbitrary Memory Access exploit/multi/browser/qtjava_pointer	2007-04-23	excellent	This module exploits an arbitrary memory access vulnerability in the Quicktime for Ja API provided with Quicktime 7. **Platforms**: osx, win **CVEs**: CVE-2007-2175 **Refs**: source
ElasticSearch Dynamic Script Arbitrary Java Execution exploit/multi/elasticsearch/script_mvel_rce	2013-12-09	excellent	This module exploits a remote command execution (RCE) vulnerability in ElasticSea exploitable by default on ElasticSearch prio 1.2.0. The bug is found in the REST API, w does not require ... **Platforms**: java **CVEs**: CVE-2014-3120 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Adobe U3D CLODProgressiveMeshDeclaration Array Overrun exploit/multi/fileformat/adobe_u3d_meshcont	2009-10-13	good	This module exploits an array overflow in A Reader and Adobe Acrobat. Affected versi include < 7.1.4, < 8.1.7, and < 9.2. By crea specially crafted pdf that a contains malfor U3D ... **Platforms**: linux, win **CVEs**: CVE-2009-2990 **Refs**: source, ref1, ref2
Ghostscript Failed Restore Command Execution exploit/multi/fileformat/ghostscript_failed_restore	2018-08-21	excellent	This module exploits a -dSAFER bypass in Ghostscript to execute arbitrary commands handling a failed restore (grestore) in PostS to disable LockSafetyParams and avoid invalidaccess. This ... **Platforms**: linux, unix, win **CVEs**: CVE-2018-16509 **Refs**: source, ref1, ref2
LibreOffice Macro Code Execution exploit/multi/fileformat/libreoffice_macro_exec	-	normal	LibreOffice comes bundled with sample ma written in Python and allows the ability to b program events to them. A macro can be ti a program event by including the script tha contains the ... **Platforms**: linux, win **CVEs**: CVE-2018-16858 **Refs**: source, ref1
Maple Maplet File Creation and Command Execution exploit/multi/fileformat/maple_maplet	2010-04-26	excellent	This module harnesses Maple's ability to c files and execute commands automatically when opening a Maplet. All versions up to are suspected vulnerable. Testing was conducted with version 13 ... **Platforms**: linux, unix, win **Refs**: source, ref1
Microsoft Office Word Malicious Macro Execution exploit/multi/fileformat/office_word_macro	2012-01-10	excellent	This module injects a malicious macro into Microsoft Office Word document (docx). Th comments field in the metadata is injected a Base64 encoded payload, which will be decoded by the macro ... **Platforms**: python, win **Refs**: source, ref1
PeaZip Zip Processing Command Injection exploit/multi/fileformat/peazip_command_injection	2009-06-05	excellent	This module exploits a command injection vulnerability in PeaZip. All versions prior to are suspected vulnerable. Testing was conducted with version 2.6.1 on Windows. order for the command ... **Platforms**: linux, unix, win **CVEs**: CVE-2009-2261 **Refs**: source, ref1
Generic Zip Slip Traversal Vulnerability exploit/multi/fileformat/zip_slip	2018-06-05	manual	This is a generic arbitrary file overwrite technique, which typically results in remote command execution. This targets a simple widespread vulnerability that has been see affecting a variety of ... **Platforms**: linux, unix, win **Refs**: source, ref1
Steamed Hams exploit/multi/hams/steamed	2018-04-01	manual	but it's a Metasploit Module. **Platforms**: android, apple_ios, bsd, java, j linux, mainframe, multi, nodejs, osx, php, python, ruby, solaris, unix, win **Refs**: source, ref1
Generic Payload Handler exploit/multi/handler	-	manual	This module is a stub that provides all of th features of the Metasploit payload system exploits that have been launched outside c framework. **Platforms**: android, apple_ios, bsd, java, j linux, mainframe, multi, nodejs, osx, php, python, ruby, solaris, unix, win **Refs**: source

Metasploit Module	Date	Rank	Details
Agent Tesla Panel Remote Code Execution exploit/multi/http/agent_tesla_panel_rce	2019-08-14	excellent	This module exploits a command injection vulnerability within the Agent Tesla control panel, in combination with an SQL injectior vulnerability and a PHP object injection vulnerability, to gain ... **Platforms**: php **Refs**: source, ref1, ref2, ref3
AjaXplorer checkInstall.php Remote Command Execution exploit/multi/http/ajaxplorer_checkinstall_exec	2010-04-04	excellent	This module exploits an arbitrary commanc execution vulnerability in the AjaXplorer 'checkInstall.php' script. All versions of AjaXplorer prior to 2.6 are vulnerable. **Platforms**: bsd, linux, osx, unix, win **Refs**: source
ActiveMQ web shell upload exploit/multi/http/apache_activemq_upload_jsp	2016-06-01	excellent	The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary fi via an HTTP PUT followed by an HTTP MC request. **Platforms**: java, linux, win **CVEs**: CVE-2016-3088 **Refs**: source, ref1
Apache Flink JAR Upload Java Code Execution exploit/multi/http/apache_flink_jar_upload_exec	2019-11-13	excellent	This module uses job functionality in Apacl Flink dashboard web interface to upload ar execute a JAR file, leading to remote exec of arbitrary Java code as the web server us This module has ... **Platforms**: java **Refs**: source, ref1, ref2, ref3, ref4
Apache Jetspeed Arbitrary File Upload exploit/multi/http/apache_jetspeed_file_upload	2016-03-06	manual	This module exploits the unsecured User Manager REST API and a ZIP file path trav in Apache Jetspeed-2, version 2.3.0 and unknown earlier versions, to upload and execute a shell. Note: this ... **Platforms**: linux, win **CVEs**: CVE-2016-0709, CVE-2016-0710 **Refs**: source, ref1, ref2, ref3
Apache NiFi API Remote Code Execution exploit/multi/http/apache_nifi_processor_rce	2020-10-03	excellent	This module uses the NiFi API to create ar ExecuteProcess processor that will execut commands. The API must be unsecured (c credentials provided) and the ExecuteProc processor must be ... **Platforms**: linux, unix, win **Refs**: source, ref1, ref2, ref3
ATutor 2.2.4 - Directory Traversal / Remote Code Execution, exploit/multi/http/atutor_upload_traversal	2019-05-17	excellent	This module exploits an arbitrary file uploa vulnerability together with a directory trave flaw in ATutor versions 2.2.4, 2.2.2 and 2.2 order to execute arbitrary commands. It firs creates ... **Platforms**: linux, win **CVEs**: CVE-2019-12169 **Refs**: source, ref1
Axis2 / SAP BusinessObjects Authenticated Code Execution (via SOAP) exploit/multi/http/axis2_deployer	2010-12-30	excellent	This module logs in to an Axis2 Web Admi Module instance using a specific user/pass uploads and executes commands via deplo a malicious web service by using SOAP. **Platforms**: java, linux, win **CVEs**: CVE-2010-0219 **Refs**: source, ref1, ref2
Cisco Prime Data Center Network Manager Arbitrary File Upload exploit/multi/http/cisco_dcnm_upload	2013-09-18	excellent	This module exploits a code execution flaw Cisco Data Center Network Manager. The vulnerability exists in processImageSave.js which can be abused through a directory traversal and a null byte ... **Platforms**: java **CVEs**: CVE-2013-5486 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
ClipBucket beats_uploader Unauthenticated Arbitrary File Upload exploit/multi/http/clipbucket_fileupload_exec	2018-03-03	excellent	This module exploits a vulnerability found i ClipBucket versions before 4.0.0 (Release 4902). A malicious file can be uploaded us an unauthenticated arbitrary file upload vulnerability. It is ... **Platforms**: php **CVEs**: CVE-2018-7665 **Refs**: source
Adobe ColdFusion CKEditor unrestricted file upload exploit/multi/http/coldfusion_ckeditor_file_upload	2018-09-11	excellent	A file upload vulnerability in the CKEditor o Adobe ColdFusion 11 (Update 14 and earli ColdFusion 2016 (Update 6 and earlier), a ColdFusion 2018 (July 12 release) allows unauthenticated remote ... **Platforms**: linux, win **CVEs**: CVE-2018-15961 **Refs**: source, ref1
Adobe ColdFusion RDS Authentication Bypass exploit/multi/http/coldfusion_rds_auth_bypass	2013-08-08	great	Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 1(allows remote attackers to bypass authentication using the RDS component. to default settings or misconfiguration, its password can be set to an empty ... **Platforms**: linux, win **CVEs**: CVE-2013-0632 **Refs**: source
Atlassian Confluence Widget Connector Macro Velocity Template Injection exploit/multi/http/confluence_widget_connector	2019-03-25	excellent	Widget Connector Macro is part of Atlassia Confluence Server and Data Center that al embed online videos, slideshows, photostr and more directly into page. A _template parameter can be used ... **Platforms**: java, linux, win **CVEs**: CVE-2019-3396 **Refs**: source, ref1, ref2, ref3
ManageEngine Eventlog Analyzer Arbitrary File Upload exploit/multi/http/eventlog_file_upload	2014-08-31	excellent	This module exploits a file upload vulnerab ManageEngine Eventlog Analyzer. The vulnerability exists in the agentUpload serv which accepts unauthenticated file uploads handles zip file ... **Platforms**: java, linux, win **CVEs**: CVE-2014-6037 **Refs**: source, ref1, ref2
Gitea Git Hooks Remote Code Execution exploit/multi/http/gitea_git_hooks_rce	2020-10-07	excellent	This module leverages an insecure setting get remote code execution on the target O the context of the user running Gitea. This possible when the current user is allowed t create `git ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-14144 **Refs**: source, ref1, ref2
Malicious Git and Mercurial HTTP Server For CVE-2014-9390 exploit/multi/http/git_client_command_exec	2014-12-18	excellent	This module exploits CVE-2014-9390, whic affects Git (versions less than 1.8.5.6, 1.9.5 2.0.5, 2.1.4 and 2.2.1) and Mercurial (versi less than 3.2.3) and describes three vulnerabilities. On ... **Platforms**: unix, win **CVEs**: CVE-2014-9390 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7, ref8
Sun/Oracle GlassFish Server Authenticated Code Execution exploit/multi/http/glassfish_deployer	2011-08-04	excellent	This module logs in to a GlassFish Server (Open Source or Commercial) using variou methods (such as authentication bypass, d credentials, or user-supplied login and dep a malicious war ... **Platforms**: java, linux, win **CVEs**: CVE-2011-0807 **Refs**: source
Gogs Git Hooks Remote Code Execution exploit/multi/http/gogs_git_hooks_rce	2020-10-07	excellent	This module leverages an insecure setting get remote code execution on the target O the context of the user running Gogs. This possible when the current user is allowed t create `git ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-14144, CVE-2020-1586 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
HorizontCMS Arbitrary PHP File Upload exploit/multi/http/horizontcms_upload_exec	2020-09-24	excellent	This module exploits an arbitrary file uploa vulnerability in HorizontCMS 1.0.0-beta in to execute arbitrary commands. The modu first attempts to authenticate to HorizontCM then tries ... **Platforms**: linux, php, win **CVEs**: CVE-2020-27387 **Refs**: source
HP SiteScope issueSiebelCmd Remote Code Execution exploit/multi/http/hp_sitescope_issuesiebelcmd	2013-10-30	great	This module exploits a code execution flaw HP SiteScope. The vulnerability exists in th APISiteScopeImpl web service, specifically the issueSiebelCmd method, which allows user to execute ... **Platforms**: unix, win **CVEs**: CVE-2013-4835 **Refs**: source
HP SiteScope Remote Code Execution exploit/multi/http/hp_sitescope_uploadfileshandler	2012-08-29	good	This module exploits a code execution flaw HP SiteScope. It exploits two vulnerabilities order to get its objective. An authentication bypass in the create operation, available through the ... **Platforms**: linux, win **CVEs**: CVE-2012-3260, CVE-2012-3261 **Refs**: source
HP System Management Homepage JustGetSNMPQueue Command Injection exploit/multi/http/hp_sys_mgmt_exec	2013-06-11	excellent	This module exploits a vulnerability found i System Management Homepage. By supp a specially crafted HTTP request, it is poss to control the 'tempfilename' variable in fun ... **Platforms**: linux, win **CVEs**: CVE-2013-3576 **Refs**: source
VMware Hyperic HQ Groovy Script-Console Java Execution exploit/multi/http/hyperic_hq_script_console	2013-10-10	excellent	This module uses the VMware Hyperic HQ Groovy script console to execute OS comn using Java. Valid credentials for an applica administrator user account are required. Th module has been ... **Platforms**: linux, unix, vbs, win **Refs**: source, ref1
Micro Focus Operations Bridge Manager Authenticated Remote Code Execution exploit/multi/http/microfocus_obm_auth_rce	2020-10-28	excellent	This module exploits an authenticated Java deserialization that affects a truckload of M Focus products: Operations Bridge Manag Application Performance Management, Da Center Automation, ... **Platforms**: java **CVEs**: CVE-2020-11853 **Refs**: source, ref1
Rocket Servergraph Admin Center fileRequestor Remote Code Execution exploit/multi/http/rocket_servergraph_file_requestor_rce	2013-10-30	great	This module abuses several directory trave flaws in Rocket Servergraph Admin Center Tivoli Storage Manager. The issues exist in fileRequestor servlet, allowing a remote att to write ... **Platforms**: linux, unix, win **CVEs**: CVE-2014-3914 **Refs**: source
Apache Struts 2 Struts 1 Plugin Showcase OGNL Code Execution exploit/multi/http/struts2_code_exec_showcase	2017-07-07	excellent	This module exploits a remote code execut vulnerability in the Struts Showcase app in Struts 1 plugin example in Struts 2.3.x seri Remote Code Execution can be performed malicious ... **Platforms**: linux, unix, win **CVEs**: CVE-2017-9791 **Refs**: source, ref1
Sun Java System Web Server WebDAV OPTIONS Buffer Overflow exploit/multi/http/sun_jsws_dav_options	2010-01-20	great	This module exploits a buffer overflow in S Java Web Server prior to version 7 Update sending an "OPTIONS" request with an ov long path, attackers can execute arbitrary In order to ... **Platforms**: linux, solaris, win **CVEs**: CVE-2010-0361 **Refs**: source

Metasploit Module	Date	Rank	Details
vBulletin widgetConfig RCE exploit/multi/http/vbulletin_widgetconfig_rce	2019-09-23	excellent	vBulletin 5.x through 5.5.4 allows remote command execution via the widgetConfig[c parameter in an ajax/render/widget_php routestring POST request. **Platforms**: php, unix, win **CVEs**: CVE-2019-16759 **Refs**: source, ref1, ref2
JBoss JMX Console Beanshell Deployer WAR Upload and Deployment exploit/multi/http/jboss_bshdeployer	2010-04-26	excellent	This module can be used to install a WAR payload on JBoss servers that have an exp "jmx-console" application. The payload is p the server by using the jboss.system:BSHDeployer's ... **Platforms**: java, linux, win **CVEs**: CVE-2010-0738 **Refs**: source, ref1, ref2
JBoss Java Class DeploymentFileRepository WAR Deployment exploit/multi/http/jboss_deploymentfilerepository	2010-04-26	excellent	This module uses the DeploymentFileRepository class in JBoss Application Server (jbossas) to deploy a JS which then deploys the WAR file. **Platforms**: java, linux, win **CVEs**: CVE-2010-0738 **Refs**: source, ref1, ref2
JBoss DeploymentFileRepository WAR Deployment (via JMXInvokerServlet) exploit/multi/http/jboss_invoke_deploy	2007-02-20	excellent	This module can be used to execute a pay on JBoss servers that have an exposed HTTPAdaptor's JMX Invoker exposed on th "JMXInvokerServlet". By invoking the meth provided by ... **Platforms**: java, linux, win **CVEs**: CVE-2007-1036 **Refs**: source, ref1
JBoss JMX Console Deployer Upload and Execute exploit/multi/http/jboss_maindeployer	2007-02-20	excellent	This module can be used to execute a pay on JBoss servers that have an exposed "jn console" application. The payload is put on server by using the jboss.system:MainDep functionality. To ... **Platforms**: java, linux, win **CVEs**: CVE-2007-1036, CVE-2010-0738 **Refs**: source, ref1, ref2
Jenkins-CI Script-Console Java Execution exploit/multi/http/jenkins_script_console	2013-01-18	good	This module uses the Jenkins-CI Groovy s console to execute OS commands using Ja **Platforms**: linux, unix, win **Refs**: source, ref1
Jenkins XStream Groovy classpath Deserialization Vulnerability exploit/multi/http/jenkins_xstream_deserialize	2016-02-24	excellent	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 . **Platforms**: linux, python, unix, win **CVEs**: CVE-2016-0792 **Refs**: source, ref1, ref2
Atlassian HipChat for Jira Plugin Velocity Template Injection exploit/multi/http/jira_hipchat_template	2015-10-28	excellent	Atlassian Hipchat is a web service for inter instant messaging. A plugin is available for that allows team collaboration at real time. message can be used to inject Java code i ... **Platforms**: java, linux, win **CVEs**: CVE-2015-5603 **Refs**: source, ref1
Atlassian Jira Authenticated Upload Code Execution exploit/multi/http/jira_plugin_upload	2018-02-22	excellent	This module can be used to execute a pay on Atlassian Jira via the Universal Plugin Manager(UPM). The module requires valid credentials to an account that has access t plugin manager. ... **Platforms**: java **Refs**: source, ref1, ref2, ref3
Mako Server v2.5, 2.6 OS Command Injection RCE exploit/multi/http/makoserver_cmd_exec	2017-09-03	excellent	This module exploits a vulnerability found i Mako Server v2.5, 2.6. It's possible to injec arbitrary OS commands in the Mako Serve tutorial page through a PUT request to sav Attacker input ... **Platforms**: unix, win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
ManageEngine Multiple Products Authenticated File Upload exploit/multi/http/manageengine_auth_upload	2014-12-15	excellent	This module exploits a directory traversal vulnerability in ManageEngine ServiceDes AssetExplorer, SupportCenter and IT360 w uploading attachment files. The JSP that accepts the upload does not ... **Platforms**: java **CVEs**: CVE-2014-5301 **Refs**: source, ref1
ManageEngine ServiceDesk Plus Arbitrary File Upload exploit/multi/http/manageengine_sd_uploader	2015-08-20	excellent	This module exploits a file upload vulnerab ManageEngine ServiceDesk Plus. The vulnerability exists in the FileUploader serv which accepts unauthenticated file uploads This module has ... **Platforms**: java **Refs**: source, ref1
ManageEngine Security Manager Plus 5.5 Build 5505 SQL Injection exploit/multi/http/manageengine_search_sqli	2012-10-18	excellent	This module exploits a SQL injection found ManageEngine Security Manager Plus advanced search page, which results in rer code execution under the context of SYST Windows, or as the user in ... **Platforms**: linux, win **Refs**: source
ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	This module exploits an unauthenticated b SQL injection in LinkViewFetchServlet, wh exposed in ManageEngine Desktop Centra build 70200 to v9 build 90033 and Passwo Manager Pro v6 ... **Platforms**: linux, win **CVEs**: CVE-2014-3996 **Refs**: source, ref1
MaraCMS Arbitrary PHP File Upload exploit/multi/http/maracms_upload_exec	2020-08-31	excellent	This module exploits an arbitrary file uploa vulnerability in MaraCMS 7.5 and prior in o to execute arbitrary commands. The modu first attempts to authenticate to MaraCMS. then tries to ... **Platforms**: linux, php, win **CVEs**: CVE-2020-25042 **Refs**: source
MediaWiki Thumb.php Remote Command Execution exploit/multi/http/mediawiki_thumb	2014-01-28	excellent	MediaWiki 1.22.x before 1.22.2, 1.21.x bef 1.21.5 and 1.19.x before 1.19.11, when DjV PDF file upload support is enabled, allows remote unauthenticated users to execute arbitrary commands via ... **Platforms**: php, unix, win **CVEs**: CVE-2014-1610 **Refs**: source, ref1, ref2
Metasploit Web UI Diagnostic Console Command Execution exploit/multi/http/metasploit_webui_console_command_execution	2016-08-23	excellent	This module exploits the "diagnostic conso feature in the Metasploit Web UI to obtain a reverse shell. The diagnostic console is ab be enabled or disabled by an administrator Metasploit ... **Platforms**: unix, win **Refs**: source
Micro Focus UCMDB Java Deserialization Unauthenticated Remote Code Execution exploit/multi/http/microfocus_ucmdb_unauth_deser	2020-10-28	excellent	This module exploits two vulnerabilities, tha when chained allow an attacker to achieve unauthenticated remote code execution in Focus UCMDB. UCMDB included in versio 2020.05 and below of ... **Platforms**: unix, win **CVEs**: CVE-2020-11853, CVE-2020-11854 **Refs**: source, ref1
Netwin SurgeFTP Remote Command Execution exploit/multi/http/netwin_surgeftp_exec	2012-12-06	good	This module exploits a vulnerability found i Netwin SurgeFTP, version 23c8 or prior. In to execute commands via the FTP service, please note that you must have a valid credential to the ... **Platforms**: unix, vbs, win **Refs**: source

Metasploit Module	Date	Rank	Details
Novell ServiceDesk Authenticated File Upload exploit/multi/http/novell_servicedesk_rce	2016-03-30	excellent	This module exploits an authenticated arbi file upload via directory traversal to execut code on the target. It has been tested on versions 6.5 and 7.1.0, in Windows and Lir installations of ... **Platforms**: linux, win **CVEs**: CVE-2016-1593 **Refs**: source, ref1, ref2
NUUO NVRmini upgrade_handle.php Remote Command Execution exploit/multi/http/nuuo_nvrmini_upgrade_rce	2018-08-04	excellent	This exploits a vulnerability in the web application of NUUO NVRmini IP camera, can be done by triggering the writeuploadd command in the upgrade_handle.php file. **Platforms**: linux, unix, win **CVEs**: CVE-2018-14933 **Refs**: source, ref1, ref2
Openfire Admin Console Authentication Bypass exploit/multi/http/openfire_auth_bypass	2008-11-10	excellent	This module exploits an authentication byp vulnerability in the administration console c Openfire servers. By using this vulnerabilit possible to upload/execute a malicious Op plugin ... **Platforms**: java, linux, win **CVEs**: CVE-2008-6508 **Refs**: source, ref1
ManageEngine OpManager and Social IT Arbitrary File Upload exploit/multi/http/opmanager_socialit_file_upload	2014-09-27	excellent	This module exploits a file upload vulnerab ManageEngine OpManager and Social IT. vulnerability exists in the FileCollector serv which accepts unauthenticated file uploads This module ... **Platforms**: java **CVEs**: CVE-2014-6034 **Refs**: source, ref1
Oracle ATS Arbitrary File Upload exploit/multi/http/oracle_ats_file_upload	2016-01-20	excellent	This module exploits an authentication byp and arbitrary file upload in Oracle Applicati Testing Suite (OATS), version 12.4.0.2.0 a unknown earlier versions, to upload and execute a JSP shell. **Platforms**: linux, win **Refs**: source
Oracle Forms and Reports Remote Code Execution exploit/multi/http/oracle_reports_rce	2014-01-15	great	This module uses two vulnerabilities in Ora Forms and Reports to get remote code execution on the host. The showenv url ca used to disclose information about a serve second vulnerability ... **Platforms**: linux, win **CVEs**: CVE-2012-3152, CVE-2012-3153 **Refs**: source
Oracle WebLogic wls-wsat Component Deserialization RCE exploit/multi/http/oracle_weblogic_wsat_deserialization_rce	2017-10-19	excellent	The Oracle WebLogic WLS WSAT Compo is vulnerable to a XML Deserialization rem code execution vulnerability. Supported ve that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and ... **Platforms**: unix, win **CVEs**: CVE-2017-10271 **Refs**: source, ref1, ref2, ref3
OrientDB 2.2.x Remote Code Execution exploit/multi/http/orientdb_exec	2017-07-13	good	This module leverages a privilege escalatic OrientDB to execute unsandboxed OS commands. All versions from 2.2.2 up to 2. should be vulnerable. **Platforms**: linux, unix, vbs, win **CVEs**: CVE-2017-11467 **Refs**: source, ref1, ref2, ref3
phpFileManager 0.9.8 Remote Code Execution exploit/multi/http/phpfilemanager_rce	2015-08-28	excellent	This module exploits a remote code execut vulnerability in phpFileManager 0.9.8 whic filesystem management tool on a single file **Platforms**: unix, win **CVEs**: CVE-2015-5958 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
PlaySMS sendfromfile.php Authenticated "Filename" Field Code Execution exploit/multi/http/playsms_filename_exec	2017-05-21	excellent	This module exploits a code injection vulnerability within an authenticated file up feature in PlaySMS v1.4. This issue is caus by improper file name handling in sendfromfile.php file. ... **Platforms**: php **CVEs**: CVE-2017-9080 **Refs**: source, ref1, ref2
PlaySMS import.php Authenticated CSV File Upload Code Execution exploit/multi/http/playsms_uploadcsv_exec	2017-05-21	excellent	This module exploits an authenticated file upload remote code excution vulnerability i PlaySMS Version 1.4. This issue is caused improper file contents handling in import.ph (aka the Phonebook ... **Platforms**: php **CVEs**: CVE-2017-9101 **Refs**: source, ref1
ProcessMaker Plugin Upload exploit/multi/http/processmaker_plugin_upload	2010-08-25	excellent	This module will generate and upload a plu to ProcessMaker resulting in execution of F code as the web server user. Credentials f valid user account with Administrator roles required to ... **Platforms**: php **Refs**: source, ref1
Apache Shiro v1.2.4 Cookie RememberME Deserial RCE exploit/multi/http/shiro_rememberme_v124_deserialize	2016-06-07	excellent	This vulnerability allows remote attackers t execute arbitrary code on vulnerable installations of Apache Shiro v1.2.4. Note t other versions of Apache Shiro may also b exploitable if the ... **Platforms**: unix, win **CVEs**: CVE-2016-4437 **Refs**: source, ref1
Simple Backdoor Shell Remote Code Execution exploit/multi/http/simple_backdoors_exec	2015-09-08	excellent	This module exploits unauthenticated simp web backdoor shells by leveraging the com backdoor shell's vulnerable parameter to execute commands. The SecLists project c Daniel Miessler and Jason ... **Platforms**: unix, win **Refs**: source, ref1, ref2
SolarWinds Storage Manager Authentication Bypass exploit/multi/http/solarwinds_store_manager_auth_filter	2014-08-19	excellent	This module exploits an authentication byp vulnerability in Solarwinds Storage Manage The vulnerability exists in the AuthenticationFilter, which allows to bypas authentication with specially ... **Platforms**: linux, win **CVEs**: CVE-2015-5371 **Refs**: source
Apache Solr Remote Code Execution via Velocity Template exploit/multi/http/solr_velocity_rce	2019-10-29	excellent	This module exploits a vulnerability in Apac Solr <= 8.3.0 which allows remote code execution via a custom Velocity template. Currently, this module only supports Solr b authentication. From ... **Platforms**: java, linux, unix, win **CVEs**: CVE-2019-17558 **Refs**: source, ref1, ref2, ref3, ref4, ref5
SonicWALL GMS 6 Arbitrary File Upload exploit/multi/http/sonicwall_gms_upload	2012-01-17	excellent	This module exploits a code execution flaw SonicWALL GMS. It exploits two vulnerabil in order to get its objective. An authenticati bypass in the Web Administration interface allows to ... **Platforms**: java, linux, win **CVEs**: CVE-2013-1359 **Refs**: source
Dell SonicWALL Scrutinizer 11.01 methodDetail SQL Injection exploit/multi/http/sonicwall_scrutinizer_methoddetail_sqli	2014-07-24	excellent	This module exploits a vulnerability found i SonicWALL Scrutinizer. The methodDetail parameter in exporters.php allows an attac write arbitrary files to the file system with a SQL ... **Platforms**: linux, win **CVEs**: CVE-2014-4977 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Splunk Search Remote Code Execution exploit/multi/http/splunk_mappy_exec	2011-12-12	excellent	This module abuses a command execution vulnerability in the web based interface of Splunk 4.2 to 4.2.4. The vulnerability exists the 'mappy' search command which allows attackers to run Python ... **Platforms**: linux, unix, win **CVEs**: CVE-2011-4642 **Refs**: source, ref1, ref2
Splunk Custom App Remote Code Execution exploit/multi/http/splunk_upload_app_exec	2012-09-27	good	'This module exploits a feature of Splunk whereby a custom application can be uploa through the web based interface. Through 'script' search command a user can call commands defined in their ... **Platforms**: linux, osx, unix, win **Refs**: source, ref1, ref2, ref3
Apache Struts Jakarta Multipart Parser OGNL Injection exploit/multi/http/struts2_content_type_ognl	2017-03-07	excellent	This module exploits a remote code execut 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 Conte Type header. Native ... **Platforms**: linux, unix, win **CVEs**: CVE-2017-5638 **Refs**: source, ref1
Apache Struts 2 Namespace Redirect OGNL Injection exploit/multi/http/struts2_namespace_ognl	2018-08-22	excellent	This module exploits a remote code execut vulnerability in Apache Struts version 2.3 - 2.3.4, and 2.5 - 2.5.16. Remote Code Exec can be performed via an endpoint that mak use of a redirect ... **Platforms**: linux, unix, win **CVEs**: CVE-2018-11776 **Refs**: source, ref1, ref2, ref3
Apache Struts 2 REST Plugin XStream RCE exploit/multi/http/struts2_rest_xstream	2017-09-05	excellent	Apache Struts versions 2.1.2 - 2.3.33 and 2.5 - Struts 2.5.12, using the REST plugin, vulnerable to a Java deserialization attack XStream library. **Platforms**: linux, python, unix, win **CVEs**: CVE-2017-9805 **Refs**: source, ref1, ref2, ref3
Apache Struts Remote Command Execution exploit/multi/http/struts_code_exec	2010-07-13	good	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 characte OGNL extensive expressions ... **Platforms**: linux, win **CVEs**: CVE-2010-1870 **Refs**: source
Apache Struts ClassLoader Manipulation Remote Code Execution exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	This module exploits a remote command execution vulnerability in Apache Struts versions 1.x (<= 1.3.10) and 2.x (< 2.3.16.2 Struts 1.x the problem is related with the ActionForm bean population ... **Platforms**: linux, win **CVEs**: CVE-2014-0094, CVE-2014-0112, C 2014-0114 **Refs**: source, ref1, ref2, ref3, ref4
Apache Struts Remote Command Execution exploit/multi/http/struts_code_exec_exception_delegator	2012-01-06	excellent	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 ... **Platforms**: java, linux, win **CVEs**: CVE-2012-0391 **Refs**: source
Apache Struts ParametersInterceptor Remote Code Execution exploit/multi/http/struts_code_exec_parameters	2011-10-01	excellent	This module exploits a remote command execution vulnerability in Apache Struts versions < 2.3.1.2. This issue is caused because the ParametersInterceptor allows the use of parentheses which in ... **Platforms**: java, linux, win **CVEs**: CVE-2011-3923 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution exploit/multi/http/struts_default_action_mapper	2013-07-02	excellent	The Struts 2 DefaultActionMapper supports method for short-circuit navigation state changes by prefixing parameters with "acti or "redirect: followed by a desired navigatic target ... **Platforms**: linux, win **CVEs**: CVE-2013-2251 **Refs**: source, ref1
Apache Struts Dynamic Method Invocation Remote Code Execution exploit/multi/http/struts_dmi_exec	2016-04-27	excellent	This module exploits a remote command execution vulnerability in Apache Struts ve between 2.3.20 and 2.3.28 (except 2.3.20.1 2.3.24.2). Remote Code Execution can be performed via method: ... **Platforms**: java, linux, win **CVEs**: CVE-2016-3081 **Refs**: source, ref1
Apache Struts REST Plugin With Dynamic Method Invocation Remote Code Execution exploit/multi/http/struts_dmi_rest_exec	2016-06-01	excellent	This module exploits a remote command execution vulnerability in Apache Struts ve between 2.3.20 and 2.3.28 (except 2.3.20.1 2.3.24.2). Remote Code Execution can be performed when using REST ... **Platforms**: java, linux, win **CVEs**: CVE-2016-3087 **Refs**: source, ref1
Apache Struts includeParams Remote Code Execution exploit/multi/http/struts_include_params	2013-05-24	great	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 ... **Platforms**: java, linux, win **CVEs**: CVE-2013-1966, CVE-2013-2115 **Refs**: source, ref1, ref2
STUNSHELL Web Shell Remote Code Execution exploit/multi/http/stunshell_exec	2013-03-23	great	This module exploits unauthenticated versi of the "STUNSHELL" web shell. This modu works when safe mode is disabled on the v server. This shell is widely used in automat RFI payloads. **Platforms**: unix, win **Refs**: source, ref1, ref2
SysAid Help Desk Administrator Portal Arbitrary File Upload exploit/multi/http/sysaid_auth_file_upload	2015-06-03	excellent	This module exploits a file upload vulnerab SysAid Help Desk. The vulnerability exists ChangePhoto.jsp in the administrator porta which does not correctly handle directory traversal ... **Platforms**: linux, win **CVEs**: CVE-2015-2994 **Refs**: source, ref1
SysAid Help Desk 'rdslogs' Arbitrary File Upload exploit/multi/http/sysaid_rdslogs_file_upload	2015-06-03	excellent	This module exploits a file upload vulnerab SysAid Help Desk v14.3 and v14.4. The vulnerability exists in the RdsLogsEntry se which accepts unauthenticated file uploads handles zip ... **Platforms**: java **CVEs**: CVE-2015-2995 **Refs**: source, ref1
Tomcat RCE via JSP Upload Bypass exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	This module uploads a jsp payload and executes it. **Platforms**: linux, win **CVEs**: CVE-2017-12617 **Refs**: source, ref1, ref2
Apache Tomcat Manager Application Deployer Authenticated Code Execution exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	This module can be used to execute a pay on Apache Tomcat servers that have an exposed "manager" application. The payloa uploaded as a WAR archive containing a js application using a PUT ... **Platforms**: java, linux, win **CVEs**: CVE-2009-3548, CVE-2009-3843, C 2009-4188, CVE-2009-4189, CVE-2010-05 CVE-2010-4094 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Apache Tomcat Manager Authenticated Upload Code Execution exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	This module can be used to execute a pay on Apache Tomcat servers that have an exposed "manager" application. The paylo uploaded as a WAR archive containing a js application using a POST ... **Platforms**: java, linux, win **CVEs**: CVE-2009-3548, CVE-2009-3843, 2009-4188, CVE-2009-4189, CVE-2010-0 CVE-2010-4094 **Refs**: source, ref1, ref2
v0pCr3w Web Shell Remote Code Execution exploit/multi/http/v0pcr3w_exec	2013-03-23	great	This module exploits a lack of authenticatic the shell developed by v0pCr3w and is wid reused in automated RFI payloads. This m takes advantage of the shell's various meth to execute ... **Platforms**: unix, win **Refs**: source, ref1, ref2
vBulletin 5.x /ajax/render/widget_tabbedcontainer_tab_panel PHP remote code execution. exploit/multi/http/vbulletin_widget_template_rce	2020-08-09	excellent	This module exploits a logic bug within the template rendering code in vBulletin 5.x. Tl module uses the vBulletin template renderi functionality to render the 'widget_tabbedcontainer_tab_panel' ... **Platforms**: php, unix, win **CVEs**: CVE-2019-16759, CVE-2020-1749 **Refs**: source, ref1
Visual Mining NetCharts Server Remote Code Execution exploit/multi/http/visual_mining_netcharts_upload	2014-11-03	excellent	This module exploits multiple vulnerabilities Visual Mining NetCharts. First, a lack of inp validation in the administration console per arbitrary jsp code upload to locations acce ... **Platforms**: linux, win **CVEs**: CVE-2014-8516 **Refs**: source
VMware vCenter Server Unauthenticated OVA File Upload RCE exploit/multi/http/vmware_vcenter_uploadova_rce	2021-02-23	manual	This module exploits an unauthenticated C file upload and path traversal in VMware vCenter Server to write a JSP payload to a accessible directory. Fixed versions are 6.5 Update 3n, 6.7 Update ... **Platforms**: linux, win **CVEs**: CVE-2021-21972 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7
vTiger CRM SOAP AddEmailAttachment Arbitrary File Upload exploit/multi/http/vtiger_soap_upload	2013-03-26	excellent	vTiger CRM allows a user to bypass authentication when requesting SOAP serv In addition, arbitrary file upload is possible through the AddEmailAttachment SOAP service. By combining both ... **Platforms**: php **CVEs**: CVE-2013-3214, CVE-2013-3215 **Refs**: source, ref1, ref2
Oracle WebLogic Server Administration Console Handle RCE exploit/multi/http/weblogic_admin_handle_rce	2020-10-20	excellent	This module exploits a path traversal and a Java class instantiation in the handle implementation of WebLogic's Administrati Console to execute code as the WebLogic Versions 10.3.6.0.0, ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-14750, CVE-2020-1488 CVE-2020-14883 **Refs**: source, ref1, ref2
WebNMS Framework Server Arbitrary File Upload exploit/multi/http/webnms_file_upload	2016-07-04	excellent	This module abuses a vulnerability in Web Framework Server 5.2 that allows an unauthenticated user to upload text files by using a directory traversal attack on the FileUploadServlet servlet. A ... **Platforms**: linux, win **CVEs**: CVE-2016-6600 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
WP Database Backup RCE exploit/multi/http/wp_db_backup_rce	2019-04-24	excellent	There exists a command injection vulnerab in the Wordpress plugin `wp-database-bac for versions < 5.2. For the backup functiona the plugin generates a `mysqldump` comm to execute. ... **Platforms**: linux, win **Refs**: source, ref1
Zemra Botnet CnC Web Panel Remote Code Execution exploit/multi/http/zemra_panel_rce	2012-06-28	excellent	This module exploits the CnC web panel of Zemra Botnet which contains a backdoor in its leaked source code. Zemra is a crimewa bot that can be used to conduct DDoS atta and is detected by ... **Platforms**: unix, win **Refs**: source, ref1, ref2, ref3
Novell ZENworks Configuration Management Arbitrary File Upload exploit/multi/http/zenworks_configuration_management_upload	2015-04-07	excellent	This module exploits a file upload vulnerab Novell ZENworks Configuration Manageme (ZCM, which is part of the ZENworks Suite The vulnerability exists in the UploadServle which accepts ... **Platforms**: java **CVEs**: CVE-2015-0779 **Refs**: source, ref1
Novell ZENworks Configuration Management Remote Execution exploit/multi/http/zenworks_control_center_upload	2013-03-22	great	This module exploits a code execution flaw Novell ZENworks Configuration Manageme SP3 and 11 SP2. The vulnerability exists in ZENworks Control Center application, allow an ... **Platforms**: linux, win **CVEs**: CVE-2013-1080 **Refs**: source, ref1
Snort 2 DCE/RPC Preprocessor Buffer Overflow exploit/multi/ids/snort_dce_rpc	2007-02-19	good	This module allows remote attackers to exe arbitrary code by exploiting the Snort servi crafted SMB traffic. The vulnerability is due boundary error within the DCE/RPC preprocessor ... **Platforms**: linux, win **CVEs**: CVE-2006-5276 **Refs**: source, ref1, ref2, ref3
Java RMI Server Insecure Default Configuration Java Code Execution exploit/multi/misc/java_rmi_server	2011-10-15	excellent	This module takes advantage of the defaul configuration of the RMI Registry and RMI Activation services, which allow loading cla from any remote (HTTP) URL. As it invoke method in the RMI ... **Platforms**: java, linux, osx, solaris, win **CVEs**: CVE-2011-3556 **Refs**: source, ref1, ref2
Western Digital Arkeia Remote Code Execution exploit/multi/misc/arkeia_agent_exec	2015-07-10	great	This module exploits a code execution flaw Western Digital Arkeia version 11.0.12 and below. The vulnerability exists in the 'arkeia daemon listening on TCP port 617. Becaus there are ... **Platforms**: unix, win **CVEs**: CVE-2015-7709 **Refs**: source, ref1
Squiggle 1.7 SVG Browser Java Code Execution exploit/multi/misc/batik_svg_java	2012-05-11	excellent	This module abuses the SVG support to execute Java Code in the Squiggle Browse included in the Batik framework 1.7 through crafted SVG file referencing a jar file. In orc gain arbitrary code ... **Platforms**: java, linux, win **Refs**: source, ref1
BMC Patrol Agent Privilege Escalation Cmd Execution exploit/multi/misc/bmc_patrol_cmd_exec	2019-01-17	excellent	This module leverages the remote comman execution feature provided by the BMC Pa Agent software. It can also be used to esca privileges on Windows hosts as the softwa runs as SYSTEM but ... **Platforms**: linux, unix, win **CVEs**: CVE-2018-20735 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
BMC Server Automation RSCD Agent NSH Remote exploit/multi/misc/bmc_server_automation_rscd_nsh_rce	2016-03-16	excellent	This module exploits a weak access contro check in the BMC Server Automation RSC agent that allows arbitrary operating syster commands to be executed without authentication. Note: Under Windows, ... **Platforms**: linux, unix, win **CVEs**: CVE-2016-1542, CVE-2016-1543 **Refs**: source, ref1, ref2, ref3
Nanopool Claymore Dual Miner APIs RCE exploit/multi/misc/claymore_dual_miner_remote_manager_rce	2018-02-09	excellent	This module takes advantage of miner rem manager APIs to exploit an RCE vulnerabi **Platforms**: linux, win **CVEs**: CVE-2018-1000049 **Refs**: source, ref1
Hashicorp Consul Remote Command Execution via Services API exploit/multi/misc/consul_service_exec	2018-08-11	excellent	This module exploits Hashicorp Consul's services API to gain remote command execution on Consul nodes. **Platforms**: linux, win **Refs**: source, ref1, ref2
Erlang Port Mapper Daemon Cookie RCE exploit/multi/misc/erlang_cookie_rce	2009-11-20	great	The erlang port mapper daemon is used to coordinate distributed erlang instances. Sh an attacker get the authentication cookie R trivial. Usually, this cookie is named ".erlang.cookie" and ... **Platforms**: linux, unix, win **Refs**: source, ref1
FreeSWITCH Event Socket Command Execution exploit/multi/misc/freeswitch_event_socket_cmd_exec	2019-11-03	excellent	This module uses the FreeSWITCH event socket interface to execute system comma using the `system` API command. The eve socket service is enabled by default and lis on TCP port 8021 on the ... **Platforms**: bsd, linux, unix, win **Refs**: source, ref1
HP Data Protector EXEC_INTEGUTIL Remote Code Execution exploit/multi/misc/hp_data_protector_exec_integutil	2014-10-02	great	This exploit abuses a vulnerability in the HI Data Protector. The vulnerability exists in tl Backup client service, which listens by defa on TCP/5555. The EXEC_INTEGUTIL requ allows to execute ... **Platforms**: unix, win **Refs**: source
IBM TM1 / Planning Analytics Unauthenticated Remote Code Execution exploit/multi/misc/ibm_tm1_unauth_rce	2019-12-19	excellent	This module exploits a vulnerability in IBM / Planning Analytics that allows an unauthenticated attacker to perform a configuration overwrite. It starts by queryin Admin server for the ... **Platforms**: linux, unix, win **CVEs**: CVE-2019-4716 **Refs**: source, ref1, ref2, ref3
Adobe IndesignServer 5.5 SOAP Server Arbitrary Script Execution exploit/multi/misc/indesign_server_soap	2012-11-11	excellent	This module abuses the "RunScript" proce provided by the SOAP interface of Adobe InDesign Server, to execute arbitrary vbscr (Windows) or applescript (OSX). The explo drops the payload on ... **Platforms**: osx, win **Refs**: source, ref1
Java Debug Wire Protocol Remote Code Execution exploit/multi/misc/java_jdwp_debugger	2010-03-12	good	This module abuses exposed Java Debug Protocol services in order to execute arbitr Java code remotely. It just abuses the prot features, since no authentication is require the service ... **Platforms**: linux, osx, win **Refs**: source, ref1, ref2, ref3, ref4, ref5
Legend Perl IRC Bot Remote Code Execution exploit/multi/misc/legend_bot_exec	2015-04-27	excellent	This module exploits a remote command execution on the Legend Perl IRC Bot. This has been used as a payload in the Shellsh spam last October 2014. This particular bo functionalities like ... **Platforms**: unix, win **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Metasploit RPC Console Command Execution exploit/multi/misc/msf_rpc_console	2011-05-22	excellent	This module connects to a specified Metas RPC server and uses the 'console.write' procedure to execute operating system commands. Valid credentials are required t access the RPC interface. This ... **Platforms**: ruby, unix, win **Refs**: source, ref1, ref2
Apache OpenOffice Text Document Malicious Macro Execution exploit/multi/misc/openoffice_document_macro	2017-02-08	excellent	This module generates an Apache OpenO Text Document with a malicious macro in it exploit successfully, the targeted user mus adjust the security level in Macro Security t either Medium or ... **Platforms**: python, win **Refs**: source, ref1
HP OpenView OmniBack II Command Execution exploit/multi/misc/openview_omniback_exec	2001-02-28	excellent	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 use the basis for this module. For ... **Platforms**: unix, win **CVEs**: CVE-2001-0311 **Refs**: source, ref1
Eclipse Equinoxe OSGi Console Command Execution exploit/multi/misc/osgi_console_exec	2018-02-13	normal	Exploit Eclipse Equinoxe OSGi (Open Serv Gateway initiative) console 'fork' command execute arbitrary commands on the remote system. **Platforms**: linux, win **Refs**: source, ref1
PHP IRC Bot pbot eval() Remote Code Execution exploit/multi/misc/pbot_exec	2009-11-02	excellent	This module allows remote command exec on the PHP IRC bot pbot by abusing the us of eval() in the implementation of the .php command. In order to work, the data to cor to the IRC server ... **Platforms**: unix, win **Refs**: source, ref1
HP Client Automation Command Injection exploit/multi/misc/persistent_hpca_radexec_exec	2014-01-02	great	This module exploits a command injection vulnerability on HP Client Automation, distributed actually as Persistent Systems Automation. The vulnerability exists in the Daemon ... **Platforms**: unix, win **CVEs**: CVE-2015-1497 **Refs**: source, ref1
Ra1NX PHP Bot PubCall Authentication Bypass Remote Code Execution exploit/multi/misc/ra1nx_pubcall_exec	2013-03-24	great	This module allows remote command exec on the PHP IRC bot Ra1NX by using the p call feature in private message to covertly bypass the authentication system. **Platforms**: unix, win **Refs**: source, ref1, ref2, ref3
TeamCity Agent XML-RPC Command Execution exploit/multi/misc/teamcity_agent_xmlrpc_exec	2015-04-14	excellent	This module allows remote code execution TeamCity Agents configured to use bidirect communication via xml-rpc. In bidirectional mode the TeamCity server pushes build commands to the Build ... **Platforms**: linux, win **Refs**: source, ref1
VERITAS NetBackup Remote Command Execution exploit/multi/misc/veritas_netbackup_cmdexec	2004-10-21	excellent	This module allows arbitrary command execution on an ephemeral port opened by Veritas NetBackup, whilst an administrator authenticated. The port is opened and allo direct console access as root ... **Platforms**: linux, unix, win **CVEs**: CVE-2004-1389 **Refs**: source
w3tw0rk / Pitbul IRC Bot Remote Code Execution exploit/multi/misc/w3tw0rk_exec	2015-06-04	excellent	This module allows remote command exec on the w3tw0rk / Pitbul IRC Bot. **Platforms**: unix, win **Refs**: source

Metasploit Module	Date	Rank	Details
Oracle Weblogic Server Deserialization RCE exploit/multi/misc/weblogic_deserialize	2018-04-17	manual	An unauthenticated attacker with network access to the Oracle Weblogic Server T3 interface can send a serialized object to th interface to execute code on vulnerable ho **Platforms**: unix, win **CVEs**: CVE-2018-2628 **Refs**: source
Oracle Weblogic Server Deserialization RCE - AsyncResponseService exploit/multi/misc/weblogic_deserialize_asyncresponseservice	2019-04-23	excellent	An unauthenticated attacker with network access to the Oracle Weblogic Server T3 interface can send a malicious SOAP requ the interface WLS AsyncResponseService execute code on the ... **Platforms**: solaris, unix, win **CVEs**: CVE-2017-10271, CVE-2019-2725 **Refs**: source, ref1, ref2, ref3
WebLogic Server Deserialization RCE - BadAttributeValueExpException exploit/multi/misc/weblogic_deserialize_badattrval	2020-01-15	normal	There exists a Java object deserialization vulnerability in multiple versions of WebLo Unauthenticated remote code execution ca achieved by sending a serialized BadAttributeValueExpException ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-2555 **Refs**: source, ref1, ref2
WebLogic Server Deserialization RCE BadAttributeValueExpException ExtComp exploit/multi/misc/weblogic_deserialize_badattr_extcomp	2020-04-30	normal	There exists a Java object deserialization vulnerability in multiple versions of WebLo Unauthenticated remote code execution ca achieved by sending a serialized ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-2883 **Refs**: source, ref1
Oracle Weblogic Server Deserialization RCE - MarshalledObject exploit/multi/misc/weblogic_deserialize_marshalledobject	2016-07-19	manual	An unauthenticated attacker with network access to the Oracle Weblogic Server T3 interface can send a serialized object (weblogic.corba.utils.MarshalledObject) to interface to execute code on ... **Platforms**: solaris, unix, win **CVEs**: CVE-2016-3510 **Refs**: source
Oracle Weblogic Server Deserialization RCE - Raw Object exploit/multi/misc/weblogic_deserialize_rawobject	2015-01-28	excellent	An unauthenticated attacker with network access to the Oracle Weblogic Server T3 interface can send a serialized object (weblogic.jms.common.StreamMessageIm the interface to execute code on ... **Platforms**: solaris, unix, win **CVEs**: CVE-2015-4852 **Refs**: source
Oracle Weblogic Server Deserialization RCE - RMI UnicastRef exploit/multi/misc/weblogic_deserialize_unicastref	2017-01-25	excellent	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 execute code on vulnerable ... **Platforms**: solaris, unix, win **CVEs**: CVE-2017-3248 **Refs**: source
Wireshark LWRES Dissector getaddrsbyname_request Buffer Overflow exploit/multi/misc/wireshark_lwres_getaddrbyname	2010-01-27	great	The LWRES dissector in Wireshark versior 0.9.15 through 1.0.10 and 1.2.0 through 1. allows remote attackers to execute arbitrar code due to a stack-based buffer overflow. bug found and ... **Platforms**: linux, osx, win **CVEs**: CVE-2010-0304 **Refs**: source, ref1, ref2
Wireshark LWRES Dissector getaddrsbyname_request Buffer Overflow (loop) exploit/multi/misc/wireshark_lwres_getaddrbyname_loop	2010-01-27	great	The LWRES dissector in Wireshark versior 0.9.15 through 1.0.10 and 1.2.0 through 1. allows remote attackers to execute arbitrar code due to a stack-based buffer overflow. bug found and ... **Platforms**: linux, osx, win **CVEs**: CVE-2010-0304 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution exploit/multi/misc/xdh_x_exec	2015-12-04	excellent	This module allows remote command exec on an IRC Bot developed by xdh. This perl was caught by Conor Patrick with his shell honeypot server and is categorized by Mar Zanke as an fBot ... **Platforms**: unix, win **Refs**: source, ref1, ref2, ref3
Zend Server Java Bridge Arbitrary Java Code Execution exploit/multi/misc/zend_java_bridge	2011-03-28	great	This module takes advantage of a trust relationship issue within the Zend Server J Bridge. The Java Bridge is responsible for handling interactions between PHP and Ja code within Zend Server. ... **Platforms**: java, win **Refs**: source
Oracle MySQL UDF Payload Execution exploit/multi/mysql/mysql_udf_payload	2009-01-16	excellent	This module creates and enables a custom (user defined function) on the target host v SELECT . into DUMPFILE method of binar injection. On default Microsoft Windows installations of MySQL ... **Platforms**: linux, win **Refs**: source, ref1
PostgreSQL COPY FROM PROGRAM Command Execution exploit/multi/postgres/postgres_copy_from_program_cmd_exec	2019-03-20	excellent	Installations running Postgres 9.3 and abo have functionality which allows for the superuser and users with 'pg_execute_server_program' to pipe to an from an external program using COPY. Thi **Platforms**: linux, osx, unix, win **CVEs**: CVE-2019-9193 **Refs**: source, ref1, ref2
PostgreSQL CREATE LANGUAGE Execution exploit/multi/postgres/postgres_createlang	2016-01-01	good	Some installations of Postgres 8 and 9 are configured to allow loading external scriptin languages. Most commonly this is Perl and Python. When enabled, command executio possible on the host. To ... **Platforms**: linux, osx, unix, win **Refs**: source, ref1, ref2, ref3
RealServer Describe Buffer Overflow exploit/multi/realserver/describe	2002-12-20	great	This module exploits a buffer overflow in RealServer 7/8/9 and was based on Johnn Cyberpunk's THCrealbad exploit. This cod should reliably exploit Linux, BSD, and Windows-based servers. **Platforms**: bsd, linux, win **CVEs**: CVE-2002-1643 **Refs**: source
SAP Solution Manager remote unauthorized OS commands execution exploit/multi/sap/cve_2020_6207_solman_rs	2020-10-03	normal	This module exploits the CVE-2020-6207 vulnerability within the SAP EEM servlet (tc~smd~agent~application~eem) of SAP Solution Manager (SolMan) running versio The vulnerability occurs due to ... **Platforms**: linux, win **CVEs**: CVE-2020-6207 **Refs**: source, ref1, ref2
SAP Management Console OSExecute Payload Execution exploit/multi/sap/sap_mgmt_con_osexec_payload	2011-03-08	excellent	This module executes an arbitrary payload through the SAP Management Console SO Interface. A valid username and password the SAP Management Console must be provided. This module has been tested ... **Platforms**: linux, win **Refs**: source, ref1
SAP SOAP RFC SXPG_CALL_SYSTEM Remote Command Execution exploit/multi/sap/sap_soap_rfc_sxpg_call_system_exec	2013-03-26	great	This module abuses the SAP NetWeaver SXPG_CALL_SYSTEM function, on the SA SOAP RFC Service, to execute remote commands. This module needs SAP crede with privileges to use the /sap/bc/soap/rfc . **Platforms**: unix, win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
SAP SOAP RFC SXPG_COMMAND_EXECUTE Remote Command Execution exploit/multi/sap/sap_soap_rfc_sxpg_command_exec	2012-05-08	great	This module abuses the SAP NetWeaver SXPG_COMMAND_EXECUTE function, o SAP SOAP RFC Service, to execute remot commands. This module needs SAP crede with privileges to use the ... **Platforms**: unix, win **Refs**: source, ref1, ref2, ref3
Inductive Automation Ignition Remote Code Execution exploit/multi/scada/inductive_ignition_rce	2020-06-11	excellent	This module exploits a Java deserializatior vulnerability in the Inductive Automation Ig SCADA product, versions 8.0.0 to (and including) 8.0.7. This exploit was tested on versions 8.0.0 and ... **Platforms**: unix, win **CVEs**: CVE-2020-10644, CVE-2020-1200 **Refs**: source, ref1, ref2, ref3
Script Web Delivery exploit/multi/script/web_delivery	2013-07-19	manual	This module quickly fires up a web server t serves a payload. The module will provide command to be run on the target machine based on the selected target. The providec command will download and ... **Platforms**: linux, osx, php, python, win **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7, ref8, ref9, ref10
VNC Keyboard Remote Code Execution exploit/multi/vnc/vnc_keyboard_exec	2015-07-10	great	This module exploits VNC servers by send virtual keyboard keys and executing a payl On Windows systems a command prompt opened and a PowerShell or CMDStager payload is typed and executed. ... **Platforms**: unix, win **Refs**: source, ref1
Tincd Post-Authentication Remote TCP Stack Buffer Overflow exploit/multi/vpn/tincd_bof	2013-04-22	average	This module exploits a stack buffer overflo Tinc's tincd service. After authentication, a specially crafted tcp packet (default port 65 leads to a buffer overflow and allows to exe ... **Platforms**: bsd, linux, offset, unix, win **CVEs**: CVE-2013-1428 **Refs**: source, ref1, ref2
Wyse Rapport Hagent Fake Hserver Command Execution exploit/multi/wyse/hagent_untrusted_hsdata	2009-07-10	excellent	This module exploits the Wyse Rapport Ha service by pretending to be a legitimate se This process involves starting both HTTP a FTP services on the attacker side, then contacting the ... **Platforms**: linux, win **CVEs**: CVE-2009-0695 **Refs**: source, ref1, ref2
Quest KACE Systems Management Command Injection exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	This module exploits a command injection vulnerability in Quest KACE Systems Management Appliance version 8.0.318 (a possibly prior). The `download_agent_installer.php` file allows unauthenticated ... **Platforms**: unix **CVEs**: CVE-2018-11138 **Refs**: source, ref1, ref2
Dogfood CRM spell.php Remote Command Execution exploit/unix/webapp/dogfood_spell_exec	2009-03-03	excellent	This module exploits a previously unpublis vulnerability in the Dogfood CRM mail func which is vulnerable to command injection i spell check feature. Because of character restrictions, ... **Platforms**: linux, unix, win **Refs**: source, ref1
Matt Wright guestbook.pl Arbitrary Command Execution exploit/unix/webapp/guestbook_ssi_exec	1999-11-05	excellent	The Matt Wright guestbook.pl <= v2.3.1 C(script contains a flaw that may allow arbitra command execution. The vulnerability requ that HTML posting is enabled in the guestbook.pl script, and ... **Platforms**: linux, unix, win **CVEs**: CVE-1999-1053 **Refs**: source

Metasploit Module	Date	Rank	Details
AdobeCollabSync Buffer Overflow Adobe Reader X Sandbox Bypass exploit/windows/local/adobe_sandbox_adobecollabsync	2013-05-14	great	This module exploits a vulnerability on Adc Reader X Sandbox. The vulnerability is du sandbox rule allowing a Low Integrity AcroRd32.exe process to write register val which can be used to ... **Platforms**: win **CVEs**: CVE-2013-2730 **Refs**: source, ref1
Agnitum Outpost Internet Security Local Privilege Escalation exploit/windows/local/agnitum_outpost_acs	2013-08-02	excellent	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 lo arbitrary DLLs through ... **Platforms**: win **Refs**: source
Microsoft Windows ALPC Task Scheduler Local Privilege Elevation exploit/windows/local/alpc_taskscheduler	2018-08-27	normal	On vulnerable versions of Windows the alp endpoint method SchRpcSetSecurity implemented by the task scheduler service be used to write arbitrary DACLs to `.job` fi located in `c:windowstasks` ... **Platforms**: win **CVEs**: CVE-2018-8440 **Refs**: source, ref1
Windows AlwaysInstallElevated MSI exploit/windows/local/always_install_elevated	2010-03-18	excellent	This module checks the AlwaysInstallEleva registry keys which dictates if .MSI files sh be installed with elevated privileges (NT AUTHORITYSYSTEM). The generated .MS has an embedded ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
Cisco AnyConnect Privilege Escalations (CVE-2020-3153 and CVE-2020-3433) exploit/windows/local/anyconnect_lpe	2020-08-05	excellent	The installer component of Cisco AnyConn Secure Mobility Client for Windows prior to 4.8.02042 is vulnerable to path traversal ar allows local attackers to create/overwrite fi arbitrary ... **Platforms**: win **CVEs**: CVE-2020-3153, CVE-2020-3433, 2020-3434 **Refs**: source, ref1, ref2, ref3
AppLocker Execution Prevention Bypass exploit/windows/local/applocker_bypass	2015-08-03	excellent	This module will generate a .NET service executable on the target and utilize InstallU run the payload bypassing the AppLocker protection. Currently only the InstallUtil me is provided, but ... **Platforms**: win **Refs**: source, ref1
AppXSvc Hard Link Privilege Escalation exploit/windows/local/appxsvc_hard_link_privesc	2019-04-09	normal	There exists a privilege escalation vulnerat for Windows 10 builds prior to build 17763. to the AppXSvc's improper handling of hard links, a user can gain full privileges over a SYSTEM-owned ... **Platforms**: win **CVEs**: CVE-2019-0841 **Refs**: source, ref1, ref2, ref3, ref4
Windows Escalate UAC Execute RunAs exploit/windows/local/ask	2012-01-03	excellent	This module will attempt to elevate executi level using the ShellExecute undocumente RunAs flag to bypass low UAC settings. **Platforms**: win **Refs**: source
SYSTEM token impersonation through NTLM bits authentication on missing WinRM Service. exploit/windows/local/bits_ntlm_token_impersonation	2019-12-06	great	This module exploit BITS behavior which tr connect to the local Windows Remote Management server (WinRM) every times starts. The module launches a fake WinRM server which listen on port 5985 ... **Platforms**: win **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
MS14-062 Microsoft Bluetooth Personal Area Networking (BthPan.sys) Privilege Escalation exploit/windows/local/bthpan	2014-07-18	average	A vulnerability within Microsoft Bluetooth Personal Area Networking module, BthPar can allow an attacker to inject memory controlled by the attacker into an arbitrary location. This can be used ... **Platforms**: win **CVEs**: CVE-2014-4971 **Refs**: source, ref1
Windows Escalate UAC Protection Bypass exploit/windows/local/bypassuac	2010-12-31	excellent	This module will bypass Windows UAC by utilizing the trusted publisher certificate thr process injection. It will spawn a second sh that has the UAC flag turned off. **Platforms**: win **Refs**: source, ref1
Windows Escalate UAC Protection Bypass (Via COM Handler Hijack) exploit/windows/local/bypassuac_comhijack	1900-01-01	excellent	This module will bypass Windows UAC by creating COM handler registry entries in th HKCU hive. When certain high integrity processes are loaded, these registry entrie referenced resulting in the ... **Platforms**: win **Refs**: source, ref1, ref2
Windows Escalate UAC Protection Bypass (Via dot net profiler) exploit/windows/local/bypassuac_dotnet_profiler	2017-03-17	excellent	Microsoft Windows allows for the automati loading of a profiling COM object during th launch of a CLR process based on certain environment variables ostensibly to monito execution. In this case, ... **Platforms**: win **Refs**: source, ref1, ref2
Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key) exploit/windows/local/bypassuac_eventvwr	2016-08-15	excellent	This module will bypass Windows UAC by hijacking a special key in the Registry unde current user hive, and inserting a custom command that will get invoked when the Windows Event Viewer is ... **Platforms**: win **Refs**: source, ref1, ref2
Windows UAC Protection Bypass (Via FodHelper Registry Key) exploit/windows/local/bypassuac_fodhelper	2017-05-12	excellent	This module will bypass Windows 10 UAC hijacking a special key in the Registry unde current user hive, and inserting a custom command that will get invoked when the Windows fodhelper.exe ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
Windows Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS exploit/windows/local/bypassuac_injection_winsxs	2017-04-06	excellent	This module will bypass Windows UAC by utilizing the trusted publisher certificate thr process injection. It will spawn a second sh that has the UAC flag turned off by abusing way "WinSxS" ... **Platforms**: win **Refs**: source, ref1
Windows Escalate UAC Protection Bypass (Via Shell Open Registry Key) exploit/windows/local/bypassuac_sdclt	2017-03-17	excellent	This module will bypass Windows UAC by hijacking a special key in the Registry unde current user hive, and inserting a custom command that will get invoked when Windo backup and restore is ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
Windows Escalate UAC Protection Bypass (Via SilentCleanup) exploit/windows/local/bypassuac_silentcleanup	2019-02-24	excellent	There's a task in Windows Task Scheduler called "SilentCleanup" which, while it's exe as Users, automatically runs with elevated privileges. When it runs, it executes the file **Platforms**: win **Refs**: source, ref1, ref2, ref3, ref4
Windows UAC Protection Bypass (Via Slui File Handler Hijack) exploit/windows/local/bypassuac_sluihijack	2018-01-15	excellent	This module will bypass UAC on Windows by hijacking a special key in the Registry u the Current User hive, and inserting a cust command that will get invoked when any b (.exe) ... **Platforms**: win **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability) exploit/windows/local/bypassuac_vbs	2015-08-22	excellent	This module will bypass Windows UAC by utilizing the missing .manifest on the script cscript/wscript.exe binaries. **Platforms**: win **Refs**: source, ref1, ref2
Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) exploit/windows/local/bypassuac_windows_store_filesys	2019-08-22	manual	This module exploits a flaw in the WSRese Windows Store Reset Tool. The tool is run the "autoElevate" property set to true, how it can be moved to a new Windows directo containing a ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry exploit/windows/local/bypassuac_windows_store_reg	2019-02-19	manual	This module exploits a flaw in the WSRese file associated with the Windows Store. Th binary has autoelevate privs, and it will run binary file contained in a low-privilege regis location. ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
Windows Capcom.sys Kernel Execution Exploit (x64 only) exploit/windows/local/capcom_sys_exec	1999-01-01	normal	This module abuses the Capcom.sys kerne driver's function that allows for an arbitrary function to be executed in the kernel from u land. This function purposely disables SME prior to invoking a ... **Platforms**: win **Refs**: source, ref1
Microsoft UPnP Local Privilege Elevation Vulnerability exploit/windows/local/comahawk	2019-11-12	excellent	This exploit uses two vulnerabilities to exec command as an elevated user. The first (C 2019-1405) uses the UPnP Device Host S to elevate to NT AUTHORITYLOCAL SER The second ... **Platforms**: win **CVEs**: CVE-2019-1322, CVE-2019-1405 **Refs**: source, ref1, ref2, ref3
PsExec via Current User Token exploit/windows/local/current_user_psexec	1999-01-01	excellent	This module uploads an executable file to t victim system, creates a share containing t executable, creates a remote service on ea target system using a UNC path to that file finally ... **Platforms**: win **CVEs**: CVE-1999-0504 **Refs**: source, ref1
LNK Code Execution Vulnerability exploit/windows/local/cve_2017_8464_lnk_lpe	2017-06-13	excellent	This module exploits a vulnerability in the handling of Windows Shortcut files (.LNK) contain a dynamic icon, loaded from a mal DLL. This vulnerability is a variant of MS15 ... **Platforms**: win **CVEs**: CVE-2015-0096, CVE-2017-8464 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Windows NtUserSetWindowFNID Win32k User Callback exploit/windows/local/cve_2018_8453_win32k_priv_esc	2018-10-09	manual	An elevation of privilege vulnerability exists Windows when the Win32k component fail properly handle objects in memory, aka "W Elevation of Privilege Vulnerability." This af Windows ... **Platforms**: win **CVEs**: CVE-2018-8453 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Microsoft Windows Uninitialized Variable Local Privilege Elevation exploit/windows/local/cve_2019_1458_wizardopium	2019-12-10	normal	This module exploits CVE-2019-1458, an arbitrary pointer dereference vulnerability v win32k which occurs due to an uninitialized variable, which allows user mode attackers write a limited ... **Platforms**: win **CVEs**: CVE-2019-1458 **Refs**: source, ref1, ref2, ref3, ref4

Metasploit Module	Date	Rank	Details
Service Tracing Privilege Elevation Vulnerability exploit/windows/local/cve_2020_0668_service_tracing	2020-02-11	excellent	This module leverages a trusted file overw with a DLL hijacking vulnerability to gain SYSTEM-level access on vulnerable Windo 10 x64 targets. **Platforms**: win **CVEs**: CVE-2020-0668 **Refs**: source, ref1, ref2, ref3, ref4, ref5
SMBv3 Compression Buffer Overflow exploit/windows/local/cve_2020_0796_smbghost	2020-03-13	good	A vulnerability exists within the Microsoft S Message Block 3.1.1 (SMBv3) protocol tha be leveraged to execute code on a vulnera server. This local exploit implementation leverages this ... **Platforms**: win **CVEs**: CVE-2020-0796 **Refs**: source, ref1, ref2
Microsoft Spooler Local Privilege Elevation Vulnerability exploit/windows/local/cve_2020_1048_printerdemon	2019-11-04	excellent	This exploit leverages a file write vulnerabi the print spooler service which will restart it stopped. Because the service cannot be stopped long enough to remove the dll, the no way to ... **Platforms**: win **CVEs**: CVE-2020-1048 **Refs**: source, ref1
Microsoft Windows DrawIconEx OOB Write Local Privilege Elevation exploit/windows/local/cve_2020_1054_drawiconex_lpe	2020-02-20	normal	This module exploits CVE-2020-1054, an o bounds write reachable from DrawIconEx v win32k. The out of bounds write can be us overwrite the pvbits of a SURFOBJ. By util this ... **Platforms**: win **CVEs**: CVE-2020-1054 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Windows Update Orchestrator unchecked ScheduleWork call exploit/windows/local/cve_2020_1313_system_orchestrator	2019-11-04	excellent	This exploit uses access to the UniversalOrchestrator ScheduleWork API which does not verify the caller's token bef scheduling a job to be run as SYSTEM. Yo cannot schedule something in a ... **Platforms**: win **CVEs**: CVE-2020-1313 **Refs**: source, ref1
Microsoft Spooler Local Privilege Elevation Vulnerability exploit/windows/local/cve_2020_1337_printerdemon	2019-11-04	excellent	This exploit leverages a file write vulnerabi the print spooler service which will restart it stopped. Because the service cannot be stopped long enough to remove the dll, the no way to ... **Platforms**: win **CVEs**: CVE-2020-1337 **Refs**: source, ref1, ref2, ref3
CVE-2020-1170 Cloud Filter Arbitrary File Creation EOP exploit/windows/local/cve_2020_17136	2020-03-10	normal	The Cloud Filter driver, cldflt.sys, on Windo 10 v1803 and later, prior to the December updates, did not set the IO_FORCE_ACCESS_CHECK or OBJ_FORCE_ACCESS_CHECK flags whe calling ... **Platforms**: win **CVEs**: CVE-2020-1170, CVE-2020-17136 **Refs**: source, ref1, ref2
Win32k ConsoleControl Offset Confusion exploit/windows/local/cve_2021_1732_win32k	2021-02-10	good	A vulnerability exists within win32k that car leveraged by an attacker to escalate privile to those of NT AUTHORITYSYSTEM. The exists in how the WndExtra field of a windo can be ... **Platforms**: win **CVEs**: CVE-2016-7255, CVE-2021-1732 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7, ref8
DnsAdmin ServerLevelPluginDll Feature Abuse Privilege Escalation exploit/windows/local/dnsadmin_serverlevelplugindll	2017-05-08	normal	This module exploits a feature in the DNS service of Windows Server. Users of the DnsAdmins group can set the `ServerLevelPluginDll` value using dnscmd to create a registry key at ... **Platforms**: win **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Docker-Credential-Wincred.exe Privilege Escalation exploit/windows/local/docker_credential_wincred	2019-07-05	manual	This exploit leverages a vulnerability in doc 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 ... **Platforms**: win **CVEs**: CVE-2019-15752 **Refs**: source, ref1
Druva inSync inSyncCPHwnet64.exe RPC Type 5 Privilege Escalation exploit/windows/local/druva_insync_insynccphwnet64_rcp_type_5_priv_esc	2020-02-25	excellent	Druva inSync client for Windows exposes a network service on TCP port 6064 on the lo network interface. inSync versions 6.6.3 an prior do not properly validate user-supplied program paths in RPC ... **CVEs**: CVE-2019-3999, CVE-2020-5752 **Refs**: source, ref1, ref2, ref3, ref4
GOG GalaxyClientService Privilege Escalation exploit/windows/local/gog_galaxyclientservice_privesc	2020-04-28	excellent	This module will send arbitrary file_paths to GOG GalaxyClientService, which will be executed with SYSTEM privileges (verified GOG Galaxy Client v1.2.62 and v2.0.12, p versions are also ... **Platforms**: win **CVEs**: CVE-2020-7352 **Refs**: source, ref1
IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL exploit/windows/local/ikeext_service	2012-10-09	good	This module exploits a missing DLL loaded the 'IKE and AuthIP Keyring Modules' (IKE service which runs as SYSTEM, and starts automatically in default installations of Vista Win8. It requires ... **Platforms**: win **Refs**: source, ref1, ref2
iPass Mobile Client Service Privilege Escalation exploit/windows/local/ipass_launch_app	2015-03-12	excellent	The named pipe, IPEFSYSPCPIPE, can be accessed by normal users to interact with t iPass service. The service provides a LaunchAppSysMode command which allow execute arbitrary commands as SYSTEM. **Platforms**: win **CVEs**: CVE-2015-0925 **Refs**: source, ref1
Lenovo System Update Privilege Escalation exploit/windows/local/lenovo_systemupdate	2015-04-12	excellent	The named pipe, SUPipeServer, can be accessed by normal users to interact with t System update service. The service provid the possibility to execute arbitrary comman SYSTEM if a valid ... **Platforms**: win **CVEs**: CVE-2015-2219 **Refs**: source, ref1
Microsoft Windows POP/MOV SS Local Privilege Elevation Vulnerability exploit/windows/local/mov_ss	2018-05-08	excellent	This module exploits a vulnerability in a statement in the system programming guid the Intel 64 and IA-32 architectures softwa developer's manual being mishandled in va operating system ... **Platforms**: win **CVEs**: CVE-2018-8897 **Refs**: source, ref1, ref2
MQAC.sys Arbitrary Write Privilege Escalation exploit/windows/local/mqac_write	2014-07-22	average	A vulnerability within the MQAC.sys modul allows an attacker to overwrite an arbitrary location in kernel memory. This module wil elevate itself to SYSTEM, then inject the payload into another ... **Platforms**: win **CVEs**: CVE-2014-4971 **Refs**: source, ref1
Windows SYSTEM Escalation via KiTrap0D exploit/windows/local/ms10_015_kitrap0d	2010-01-19	great	This module will create a new session with SYSTEM privileges via the KiTrap0D explo Tavis Ormandy. If the session in use is alre elevated then the exploit will not run. The module relies on ... **Platforms**: win **CVEs**: CVE-2010-0232 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Windows Escalate Task Scheduler XML Privilege Escalation exploit/windows/local/ms10_092_schelevator	2010-09-13	excellent	This module exploits the Task Scheduler 2 XML 0day exploited by Stuxnet. When processing task files, the Windows Task Scheduler only uses a CRC32 checksum t validate that the file has not been ... **Platforms**: win **CVEs**: CVE-2010-3338 **Refs**: source
MS11-080 AfdJoinLeaf Privilege Escalation exploit/windows/local/ms11_080_afdjoinleaf	2011-11-30	average	This module exploits a flaw in the AfdJoinL function of the afd.sys driver to overwrite d kernel space. An address within the HalDispatchTable is overwritten and when triggered with a call ... **Platforms**: win **Refs**: source
MS13-005 HWND_BROADCAST Low to Medium Integrity Privilege Escalation exploit/windows/local/ms13_005_hwnd_broadcast	2012-11-27	excellent	Due to a problem with isolating window broadcast messages in the Windows kerne attacker can broadcast commands from a l Integrity Level process to a higher Integrity Level process, thereby ... **Platforms**: win **CVEs**: CVE-2013-0008 **Refs**: source, ref1
Windows NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei) exploit/windows/local/ms13_053_schlamperei	2013-12-01	average	This module leverages a kernel pool overfl Win32k which allows local privilege escalat The kernel shellcode nulls the ACL for the winlogon.exe process (a SYSTEM process This allows any ... **Platforms**: win **CVEs**: CVE-2013-1300 **Refs**: source, ref1
Windows TrackPopupMenuEx Win32k NULL Page exploit/windows/local/ms13_081_track_popup_menu	2013-10-08	average	This module exploits a vulnerability in win32k.sys where under specific conditions TrackPopupMenuEx will pass a NULL poin the MNEndMenuState procedure. This mo has been tested successfully ... **Platforms**: win **CVEs**: CVE-2013-3881 **Refs**: source, ref1, ref2
MS13-097 Registry Symlink IE Sandbox Escape exploit/windows/local/ms13_097_ie_registry_symlink	2013-12-10	great	This module exploits a vulnerability in Inter Explorer Sandbox which allows to escape f Enhanced Protected Mode and execute co with Medium Integrity. The vulnerability exi the ... **Platforms**: win **CVEs**: CVE-2013-5045 **Refs**: source, ref1
MS14-009 .NET Deployment Service IE Sandbox Escape exploit/windows/local/ms14_009_ie_dfsvc	2014-02-11	great	This module abuses a process creation po Internet Explorer's sandbox, specifically in .NET Deployment Service (dfsvc.exe), whi allows the attacker to escape the Enhance Protected Mode, ... **Platforms**: win **CVEs**: CVE-2014-0257 **Refs**: source, ref1
Windows TrackPopupMenu Win32k NULL Pointer Dereference exploit/windows/local/ms14_058_track_popup_menu	2014-10-14	normal	This module exploits a NULL Pointer Dereference in win32k.sys, the vulnerabilit be triggered through the use of TrackPopupMenu. Under special condition NULL pointer dereference can be ... **Platforms**: win **CVEs**: CVE-2014-4113 **Refs**: source, ref1
MS14-070 Windows tcpip!SetAddrOptions NULL Pointer Dereference exploit/windows/local/ms14_070_tcpip_ioctl	2014-11-11	average	A vulnerability within the Microsoft TCP/IP protocol driver tcpip.sys can allow a local attacker to trigger a NULL pointer derefere by using a specially crafted IOCTL. This fla can be abused to ... **Platforms**: win **CVEs**: CVE-2014-4076 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
MS15-004 Microsoft Remote Desktop Services Web Proxy IE Sandbox Escape exploit/windows/local/ms15_004_tswbproxy	2015-01-13	good	This module abuses a process creation po Internet Explorer's sandbox, specifically, Microsoft's RemoteApp and Desktop Connections runtime proxy, TSWbPrxy.exe vulnerability allows the ... **Platforms**: win **CVEs**: CVE-2015-0016 **Refs**: source, ref1
Windows ClientCopyImage Win32k Exploit exploit/windows/local/ms15_051_client_copy_image	2015-05-12	normal	This module exploits improper object hand the win32k.sys kernel mode driver. This mo has been tested on vulnerable builds of Windows 7 x64 and x86, and Windows 200 SP1 x64. **Platforms**: win **CVEs**: CVE-2015-1701 **Refs**: source, ref1, ref2, ref3
MS15-078 Microsoft Windows Font Driver Buffer Overflow exploit/windows/local/ms15_078_atmfd_bof	2015-07-11	manual	This module exploits a pool based buffer overflow in the atmfd.dll driver when parsin malformed font. The vulnerability was explo by the hacking team and disclosed in the J data leak. This ... **Platforms**: win **CVEs**: CVE-2015-2426, CVE-2015-2433 **Refs**: source, ref1, ref2, ref3, ref4
Windows Escalate UAC Protection Bypass (In Memory Injection) exploit/windows/local/bypassuac_injection	2010-12-31	excellent	This module will bypass Windows UAC by utilizing the trusted publisher certificate thro process injection. It will spawn a second sh that has the UAC flag turned off. This modu uses the ... **Platforms**: win **Refs**: source, ref1, ref2
Background Intelligent Transfer Service Arbitrary File Move Privilege Elevation Vulnerability exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move	2020-03-10	excellent	This module exploits CVE-2020-0787, an arbitrary file move vulnerability in outdated versions of the Background Intelligent Tran Service (BITS), to overwrite ... **Platforms**: win **CVEs**: CVE-2020-0688, CVE-2020-0787 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref
Micro Focus Operations Bridge Manager Local Privilege Escalation exploit/windows/local/microfocus_operations_privesc	2020-10-28	excellent	This module exploits an incorrectly permissioned folder in Micro Focus Operat Bridge Manager. An unprivileged user (suc Guest) can drop a JSP file in an exploded ' directory and then access ... **Platforms**: win **CVEs**: CVE-2020-11858 **Refs**: source, ref1
Windows WMI Receive Notification Exploit exploit/windows/local/ms16_014_wmi_recv_notif	2015-12-04	normal	This module exploits an uninitialized stack variable in the WMI subsystem of ntoskrnl. module has been tested on vulnerable buil Windows 7 SP0 x64 and Windows 7 SP1 x **Platforms**: win **CVEs**: CVE-2016-0040 **Refs**: source, ref1, ref2, ref3
Windows Persistent Service Installer exploit/windows/local/persistence_service	2018-10-20	excellent	This Module will generate and upload an executable to a remote host, next will make persistent service. It will create a new serv which will start the payload whenever the service is running. ... **Platforms**: win **Refs**: source, ref1
MS16-016 mrxdav.sys WebDav Local Privilege Escalation exploit/windows/local/ms16_016_webdav	2016-02-09	excellent	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 AUTHORITYSYSTEM before executing the **Platforms**: win **CVEs**: CVE-2016-0051 **Refs**: source

Metasploit Module	Date	Rank	Details
MS16-032 Secondary Logon Handle Privilege Escalation exploit/windows/local/ms16_032_secondary_logon_handle_privesc	2016-03-21	normal	This module exploits the lack of sanitizatio standard handles in Windows' Secondary L Service. The vulnerability is known to affec versions of Windows 7-10 and 2k8-2k12 32 64 bit. This ... **Platforms**: win **CVEs**: CVE-2016-0099 **Refs**: source, ref1, ref2
Windows Net-NTLMv2 Reflection DCOM/RPC exploit/windows/local/ms16_075_reflection	2016-01-16	normal	Module utilizes the Net-NTLMv2 reflection between DCOM/RPC to achieve a SYSTE handle for elevation of privilege. Currently t module does not spawn as SYSTEM, howe once achieving a shell, one ... **Platforms**: win **CVEs**: CVE-2014-4113, CVE-2016-3225 **Refs**: source, ref1, ref2, ref3
Windows Net-NTLMv2 Reflection DCOM/RPC (Juicy) exploit/windows/local/ms16_075_reflection_juicy	2016-01-16	great	This module utilizes the Net-NTLMv2 reflec between DCOM/RPC to achieve a SYSTE handle for elevation of privilege. It requires CLSID string. Windows 10 after version 18 (April 2018 update, ... **Platforms**: win **CVEs**: CVE-2014-4113, CVE-2016-3225 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Windows SetImeInfoEx Win32k NULL Pointer Dereference exploit/windows/local/ms18_8120_win32k_privesc	2018-05-09	good	This module exploits elevation of privilege vulnerability that exists in Windows 7 and 2 R2 when the Win32k component fails to properly handle objects in memory. An atta who successfully ... **Platforms**: win **CVEs**: CVE-2018-8120 **Refs**: source, ref1, ref2, ref3, ref4
MS14-002 Microsoft Windows ndproxy.sys Local Privilege Escalation exploit/windows/local/ms_ndproxy	2013-11-27	average	This module exploits a flaw in the ndproxy. driver on Windows XP SP3 and Windows 2 SP2 systems, exploited in the wild in Nove 2013. The vulnerability exists while proces an IO Control ... **Platforms**: win **CVEs**: CVE-2013-5065 **Refs**: source
Novell Client 2 SP3 nicm.sys Local Privilege Escalation exploit/windows/local/novell_client_nicm	2013-05-22	average	This module exploits a flaw in the nicm.sys driver to execute arbitrary code in kernel sp The vulnerability occurs while handling ioct requests with code 0x143B6B, where a use provided pointer ... **Platforms**: win **CVEs**: CVE-2013-3956 **Refs**: source, ref1, ref2
Novell Client 4.91 SP4 nwfs.sys Local Privilege Escalation exploit/windows/local/novell_client_nwfs	2008-06-26	average	This module exploits a flaw in the nwfs.sys driver to overwrite data in kernel space. Th corruption occurs while handling ioctl reque with code 0x1438BB, where a 0x0000000 dword is written to an ... **Platforms**: win **CVEs**: CVE-2008-3158 **Refs**: source
MS15-001 Microsoft Windows NtApphelpCacheControl Improper Authorization Check exploit/windows/local/ntapphelpcachecontrol	2014-09-30	normal	On Windows, the system call NtApphelpCacheControl (the code is actua ahcache.sys) allows application compatibil data to be cached for quick reuse when ne processes are created. A normal ... **Platforms**: win **CVEs**: CVE-2015-0002 **Refs**: source, ref1
Microsoft Windows NtUserMNDragOver Local Privilege Elevation exploit/windows/local/ntusermndragover	2019-03-12	normal	This module exploits a NULL pointer dereference vulnerability in MNGetpItemFromIndex(), which is reachab via a NtUserMNDragOver() system call. Th NULL pointer dereference occurs because ... **Platforms**: win **CVEs**: CVE-2019-0808 **Refs**: source, ref1, ref2, ref3, ref4

Metasploit Module	Date	Rank	Details
Nvidia (nvsvc) Display Driver Service Local Privilege Escalation exploit/windows/local/nvidia_nvsvc	2012-12-25	average	The named pipe, pipensvr, has a NULL DA allowing any authenticated user to interact the service. It contains a stacked based bu overflow as a result of a memmove operati Note the slight ... **Platforms**: win **CVEs**: CVE-2013-0109 **Refs**: source, ref1
Panda Security PSEvents Privilege Escalation exploit/windows/local/panda_psevents	2016-06-27	excellent	PSEvents.exe within several Panda Securi products runs hourly with SYSTEM privileg When run, it checks a user writable folder f certain DLL files, and if any are found they automatically ... **Platforms**: win **Refs**: source, ref1, ref2
Windows Manage Memory Payload Injection exploit/windows/local/payload_inject	2011-10-12	excellent	This module will inject a payload into mem a process. If a payload isn't selected, then default to a reverse x86 TCP meterpreter. I PID datastore option isn't specified, then it' **Platforms**: win **Refs**: source
Windows Persistent Registry Startup Payload Installer exploit/windows/local/persistence	2011-10-19	excellent	This module will install a payload that is executed during boot. It will be executed ei at user logon or system startup via the regi value in "CurrentVersionRun" (depending c privilege and ... **Platforms**: win **Refs**: source
Windows Silent Process Exit Persistence exploit/windows/local/persistence_image_exec_options	2008-06-28	excellent	Windows allows you to set up a debug pro when a process exits. This module uploads payload and declares that it is the debug process to launch when a specified proces exits. **Platforms**: win **Refs**: source, ref1, ref2
Plantronics Hub SpokesUpdateService Privilege Escalation exploit/windows/local/plantronics_hub_spokesupdateservice_privesc	2019-08-30	excellent	The Plantronics Hub client application for Windows makes use of an automatic upda service `SpokesUpdateService.exe` which automatically executes a file specified in th `MajorUpgrade.config` ... **Platforms**: win **CVEs**: CVE-2019-15742 **Refs**: source, ref1
Windows Command Shell Upgrade (Powershell) exploit/windows/local/powershell_cmd_upgrade	1999-01-01	excellent	This module executes Powershell to upgra Windows Shell session to a full Meterprete session. **Platforms**: win **Refs**: source
Powershell Remoting Remote Command Execution exploit/windows/local/powershell_remoting	1999-01-01	excellent	This module uses Powershell Remoting (T 47001) to inject payloads on target machin RHOSTS are specified, it will try to resolve IPs to hostnames, otherwise use a HOSTF to supply a list ... **Platforms**: win **CVEs**: CVE-1999-0504 **Refs**: source
Windows EPATHOBJ::pprFlattenRec Local Privilege Escalation exploit/windows/local/ppr_flatten_rec	2013-05-15	average	This module exploits a vulnerability on EPATHOBJ::pprFlattenRec due to the usag uninitialized data which allows to corrupt memory. At the moment, the module has b tested successfully on ... **Platforms**: win **CVEs**: CVE-2013-3660 **Refs**: source, ref1
Powershell Payload Execution exploit/windows/local/ps_persist	2012-08-14	excellent	This module generates a dynamic executa on the session host using .NET templates. is pulled from C# templates and impregnat with a payload before being sent to a modi PowerShell session ... **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
Authenticated WMI Exec via Powershell exploit/windows/local/ps_wmi_exec	2012-08-19	excellent	This module uses WMI execution to launch payload instance on a remote machine. In to avoid AV detection, all execution is perfo in memory via psh-net encoded payload. Persistence option ... **Platforms**: win **Refs**: source
PXE Exploit Server exploit/windows/local/pxeexploit	2011-08-05	excellent	This module provides a PXE server, runnin DHCP and TFTP server. The default configuration loads a linux kernel and initrd memory that reads the hard drive, placing t payload on the hard ... **Platforms**: win **Refs**: source
Razer Synapse rzpnk.sys ZwOpenProcess exploit/windows/local/razer_zwopenprocess	2017-03-22	normal	A vulnerability exists in the latest version o Razer Synapse (v2.20.15.1104 as of the da disclosure) which can be leveraged locally malicious application to elevate its privilege those ... **Platforms**: win **CVEs**: CVE-2017-9769 **Refs**: source, ref1
Windows Registry Only Persistence exploit/windows/local/registry_persistence	2015-07-01	excellent	This module will install a payload that is executed during boot. It will be executed ei at user logon or system startup via the regi value in "CurrentVersionRun" (depending o privilege and ... **Platforms**: win **Refs**: source
Ricoh Driver Privilege Escalation exploit/windows/local/ricoh_driver_privesc	2020-01-22	normal	Various Ricoh printer drivers allow escalati privileges on Windows systems. For vulner drivers, a low-privileged user can read/write within the `RICOH_DRV` directory and its . **Platforms**: win **CVEs**: CVE-2019-19363 **Refs**: source, ref1
Windows Run Command As User exploit/windows/local/run_as	1999-01-01	excellent	This module will login with the specified username/password and execute the supp command as a hidden process. Output is r returned by default. Unless targeting a loca user either set the ... **Platforms**: win **Refs**: source, ref1
Windows Manage User Level Persistent Payload Installer exploit/windows/local/s4u_persistence	2013-01-02	excellent	Creates a scheduled task that will run using service-for-user (S4U). This allows the scheduled task to run even as an unprivileg user that is not logged into the device. This result in lower ... **Platforms**: win **Refs**: source, ref1, ref2
Windows Escalate Service Permissions Local Privilege Escalation exploit/windows/local/service_permissions	2012-10-15	great	This module attempts to exploit existing administrative privileges to obtain a SYSTE session. If directly creating a service fails, t module will inspect existing services to loo insecure ... **Platforms**: win **Refs**: source, ref1
Windows Server 2012 SrClient DLL hijacking exploit/windows/local/srclient_dll_hijacking	2021-02-19	excellent	All editions of Windows Server 2012 (but n 2012 R2) are vulnerable to DLL hijacking d the way TiWorker.exe will try to call the non existent `SrClient.dll` file when Windows U checks for ... **Platforms**: win **Refs**: source, ref1
Windows Unquoted Service Path Privilege Escalation exploit/windows/local/unquoted_service_path	2001-10-25	excellent	This module exploits a logic flaw due to ho lpApplicationName parameter is handled. \ the lpApplicationName contains a space, th name is ambiguous. Take this file path as example: ... **Platforms**: win **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
VirtualBox Guest Additions VBoxGuest.sys Privilege Escalation exploit/windows/local/virtual_box_guest_additions	2014-07-15	average	A vulnerability within the VBoxGuest driver allows an attacker to inject memory they co into an arbitrary location they define. This c be used by an attacker to overwrite HalDispatchTable+0x4 ... **Platforms**: win **CVEs**: CVE-2014-2477 **Refs**: source, ref1
VirtualBox 3D Acceleration Virtual Machine Escape exploit/windows/local/virtual_box_opengl_escape	2014-03-11	average	This module exploits a vulnerability in the 3 Acceleration support for VirtualBox. The vulnerability exists in the remote rendering OpenGL-based 3D graphics. By sending a sequence of specially ... **Platforms**: win **CVEs**: CVE-2014-0983 **Refs**: source, ref1, ref2
Persistent Payload in Windows Volume Shadow Copy exploit/windows/local/vss_persistence	2011-10-21	excellent	This module will attempt to create a persist payload in a new volume shadow copy. Th based on the VSSOwn Script originally pos by Tim Tomes and Mark Baggett. This moc has been tested ... **Platforms**: win **Refs**: source, ref1, ref2
WebEx Local Service Permissions Exploit exploit/windows/local/webexec	2018-10-09	good	This module exploits a flaw in the 'webexservice' Windows service, which rur SYSTEM, can be used to run arbitrary commands locally, and can be started by li users in default installations. **Platforms**: win **CVEs**: CVE-2018-15442 **Refs**: source, ref1
Windscribe WindscribeService Named Pipe Privilege Escalation exploit/windows/local/windscribe_windscribeservice_priv_esc	2018-05-24	excellent	The Windscribe VPN client application for Windows makes use of a Windows service `WindscribeService.exe` which exposes a named pipe `\.pipeWindscribeService` allo execution of programs with ... **Platforms**: win **CVEs**: CVE-2018-11479 **Refs**: source, ref1, ref2
Windows Management Instrumentation (WMI) Remote Command Execution exploit/windows/local/wmi	1999-01-01	excellent	This module executes powershell on the re host using the current user credentials or tl supplied. Instead of using PSEXEC over T port 445 we use the WMIC command to sta Remote Procedure ... **Platforms**: win **CVEs**: CVE-1999-0504 **Refs**: source, ref1
WMI Event Subscription Persistence exploit/windows/local/wmi_persistence	2017-06-06	normal	This module will create a permanent WMI subscription to achieve file-less persistenc using one of five methods. The EVENT me will create an event filter that will query the event log for ... **Platforms**: win **Refs**: source, ref1, ref2
Symantec System Center Alert Management System (hndlrsvc.exe) Arbitrary Command Execution exploit/windows/antivirus/ams_hndlrsvc	2010-07-26	excellent	Symantec System Center Alert Manageme System is prone to a remote command-inje vulnerability because the application fails t properly sanitize user-supplied input. This part of Symantec ... **Platforms**: win **CVEs**: CVE-2010-0111 **Refs**: source, ref1
Symantec System Center Alert Management System (xfr.exe) Arbitrary Command Execution exploit/windows/antivirus/ams_xfr	2009-04-28	excellent	Symantec System Center Alert Manageme System is prone to a remote command-inje vulnerability because the application fails t properly sanitize user-supplied input. **Platforms**: win **CVEs**: CVE-2009-1429 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Symantec Endpoint Protection Manager /servlet/ConsoleServlet Remote Command Execution exploit/windows/antivirus/symantec_endpoint_manager_rce	2014-02-24	excellent	This module exploits XXE and SQL injectic flaws in Symantec Endpoint Protection Ma versions 11.0, 12.0 and 12.1. When supply specially crafted XML external entity (XXE) request an attacker ... **Platforms**: win **CVEs**: CVE-2013-5014, CVE-2013-5015 **Refs**: source, ref1
Symantec Alert Management System Intel Alert Originator Service Buffer Overflow exploit/windows/antivirus/symantec_iao	2009-04-28	good	This module exploits a stack buffer overflo Intel Alert Originator Service msgsys.exe. V an attacker sends a specially crafted alert, arbitrary code may be executed. **Platforms**: win **CVEs**: CVE-2009-1430 **Refs**: source
Symantec Remote Management Buffer Overflow exploit/windows/antivirus/symantec_rtvscan	2006-05-24	good	This module exploits a stack buffer overflo Symantec Client Security 3.0.x. This modu has only been tested against Symantec Cli Security 3.0.2 build 10.0.2.2000. **Platforms**: win **CVEs**: CVE-2006-2630 **Refs**: source, ref1
Symantec Workspace Streaming ManagementAgentServer.putFile XMLRPC Request Arbitrary File Upload exploit/windows/antivirus/symantec_workspace_streaming_exec	2014-05-12	excellent	This module exploits a code execution flaw Symantec Workspace Streaming. The vulnerability exists in the ManagementAgentServer.putFile XMLRPC exposed by the as_agent.exe service, whic allows ... **Platforms**: java **CVEs**: CVE-2014-1649 **Refs**: source, ref1
Trend Micro ServerProtect 5.58 Buffer Overflow exploit/windows/antivirus/trendmicro_serverprotect	2007-02-20	good	This module exploits a buffer overflow in Tr Micro ServerProtect 5.58 Build 1060. By sending a specially crafted RPC request, a attacker could overflow the buffer and exec arbitrary code. **Platforms**: win **CVEs**: CVE-2007-1070 **Refs**: source
Trend Micro ServerProtect 5.58 CreateBinding() Buffer Overflow exploit/windows/antivirus/trendmicro_serverprotect_createbinding	2007-05-07	good	This module exploits a buffer overflow in Tr Micro ServerProtect 5.58 Build 1060. By sending a specially crafted RPC request, a attacker could overflow the buffer and exec arbitrary code. **Platforms**: win **CVEs**: CVE-2007-2508 **Refs**: source
Trend Micro ServerProtect 5.58 EarthAgent.EXE Buffer Overflow exploit/windows/antivirus/trendmicro_serverprotect_earthagent	2007-05-07	good	This module exploits a buffer overflow in Tr Micro ServerProtect 5.58 Build 1060 EarthAgent.EXE. By sending a specially cr RPC request, an attacker could overflow th buffer and execute ... **Platforms**: win **CVEs**: CVE-2007-2508 **Refs**: source
Arkeia Backup Client Type 77 Overflow (Win32) exploit/windows/arkeia/type77	2005-02-18	good	This module exploits a stack buffer overflo the Arkeia backup client for the Windows platform. This vulnerability affects all versic up to and including 5.3.3. **Platforms**: win **CVEs**: CVE-2005-0491 **Refs**: source, ref1
Energizer DUO USB Battery Charger Arucer.dll Trojan Code Execution exploit/windows/backdoor/energizer_duo_payload	2010-03-05	excellent	This module will execute an arbitrary paylo against any system infected with the Arugi trojan horse. This backdoor was shipped w the software package accompanying the Energizer DUO USB ... **Platforms**: win **CVEs**: CVE-2010-0103 **Refs**: source

Metasploit Module	Date	Rank	Details
Veritas Backup Exec Name Service Overflow exploit/windows/backupexec/name_service	2004-12-16	average	This module exploits a vulnerability in the Veritas Backup Exec Agent Browser servic This vulnerability occurs when a recv() call a length value too long for the destination s buffer. By ... **Platforms**: win **CVEs**: CVE-2004-1172 **Refs**: source, ref1
Veritas Backup Exec Windows Remote Agent Overflow exploit/windows/backupexec/remote_agent	2005-06-22	great	This module exploits a stack buffer overflo the Veritas BackupExec Windows Agent software. This vulnerability occurs when a authentication request is received with type and a long ... **Platforms**: win **CVEs**: CVE-2005-0773 **Refs**: source, ref1
Veritas/Symantec Backup Exec SSL NDMP Connection Use-After-Free exploit/windows/backupexec/ssl_uaf	2017-05-10	normal	This module exploits a use-after-free vulnerability in the handling of SSL NDMP connections in Veritas/Symantec Backup E Remote Agent for Windows. When SSL is established on a NDMP connection ... **Platforms**: win **CVEs**: CVE-2017-8895 **Refs**: source, ref1
Computer Associates ARCserve REPORTREMOTEEXECUTECML Buffer Overflow exploit/windows/brightstor/ca_arcserve_342	2008-10-09	average	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 ... **Platforms**: win **CVEs**: CVE-2008-4397 **Refs**: source, ref1
CA BrightStor Discovery Service TCP Overflow exploit/windows/brightstor/discovery_tcp	2005-02-14	average	This module exploits a vulnerability in the C BrightStor Discovery Service. This vulnera occurs when a specific type of request is s the TCP listener on port 41523. This vulnerability ... **Platforms**: win **CVEs**: CVE-2005-2535 **Refs**: source, ref1
CA BrightStor Discovery Service Stack Buffer Overflow exploit/windows/brightstor/discovery_udp	2004-12-20	average	This module exploits a vulnerability in the C BrightStor Discovery Service. This vulnera occurs when a large request is sent to UDF 41524, triggering a stack buffer overflow. **Platforms**: win **CVEs**: CVE-2005-0260 **Refs**: source, ref1
Computer Associates Alert Notification Buffer Overflow exploit/windows/brightstor/etrust_itm_alert	2008-04-04	average	This module exploits a buffer overflow in Computer Associates Threat Manager for t Enterprise r8.1 By sending a specially craft RPC request, an attacker could overflow th buffer and execute ... **Platforms**: win **CVEs**: CVE-2007-4620 **Refs**: source
CA BrightStor HSM Buffer Overflow exploit/windows/brightstor/hsmserver	2007-09-27	great	This module exploits one of the multiple sta buffer overflows in Computer Associates BrightStor HSM. By sending a specially cra request, an attacker could overflow the buf and execute ... **Platforms**: win **CVEs**: CVE-2007-5082 **Refs**: source
CA BrightStor ARCserve for Laptops and Desktops LGServer Buffer Overflow exploit/windows/brightstor/lgserver	2007-01-31	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup for Laptops Desktops 11.1. By sen a specially crafted request, an attacker cou overflow the ... **Platforms**: win **CVEs**: CVE-2007-0449 **Refs**: source

Metasploit Module	Date	Rank	Details
CA BrightStor ARCserve for Laptops and Desktops LGServer Multiple Commands Buffer Overflow exploit/windows/brightstor/lgserver_multi	2007-06-06	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup for Laptops Desktops 11.1. By sen a specially crafted request to multiple commands, an attacker ... **Platforms**: win **CVEs**: CVE-2007-3216 **Refs**: source
CA BrightStor ARCserve for Laptops and Desktops LGServer Buffer Overflow exploit/windows/brightstor/lgserver_rxrlogin	2007-06-06	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup for Laptops Desktops 11.1. By sen a specially crafted request, an attacker cou overflow the ... **Platforms**: win **CVEs**: CVE-2007-5003 **Refs**: source
CA BrightStor ARCserve for Laptops and Desktops LGServer rxsSetDataGrowthScheduleAndFilter Buffer Overflow exploit/windows/brightstor/lgserver_rxssetdatagrowthscheduleandfilter	2007-06-06	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup for Laptops Desktops 11.1. By sen a specially crafted request (rxsSetDataGrowthScheduleAndFilter ... **Platforms**: win **CVEs**: CVE-2007-3216 **Refs**: source
CA BrightStor ARCserve for Laptops and Desktops LGServer Buffer Overflow exploit/windows/brightstor/lgserver_rxsuselicenseini	2007-06-06	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup for Laptops Desktops 11.1. By sen a specially crafted request (rxsUseLicense an attacker ... **Platforms**: win **CVEs**: CVE-2007-3216 **Refs**: source
CA BrightStor ARCserve License Service GCR NETWORK Buffer Overflow exploit/windows/brightstor/license_gcr	2005-03-02	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup 11.0. By sending a specially crafte request to the lic98rmtd.exe service, an att could overflow ... **Platforms**: win **CVEs**: CVE-2005-0581 **Refs**: source
CA BrightStor ArcServe Media Service Stack Buffer Overflow exploit/windows/brightstor/mediasrv_sunrpc	2007-04-25	average	This exploit targets a stack buffer overflow MediaSrv RPC service of CA BrightStor ARCserve. By sending a specially crafted SUNRPC request, an attacker can overflo stack buffer and execute ... **Platforms**: win **CVEs**: CVE-2007-2139 **Refs**: source
CA BrightStor ARCserve Message Engine Buffer Overflow exploit/windows/brightstor/message_engine	2007-01-11	average	This module exploits a buffer overflow in Computer Associates BrightStor ARCserve Backup 11.1 - 11.5 SP2. By sending a spe crafted RPC request, an attacker could ov the buffer and execute ... **Platforms**: win **CVEs**: CVE-2007-0169 **Refs**: source
CA BrightStor ARCserve Message Engine 0x72 Buffer Overflow exploit/windows/brightstor/message_engine_72	2010-10-04	average	This module exploits a buffer overflow in Computer Associates BrightStor ARCserve Backup 11.1 - 11.5 SP2. By sending a spe crafted RPC request, an attacker could ov the buffer and execute ... **Platforms**: win **Refs**: source, ref1
CA BrightStor ARCserve Message Engine Heap Overflow exploit/windows/brightstor/message_engine_heap	2006-10-05	average	This module exploits a heap overflow in Computer Associates BrightStor ARCserve Backup 11.5. By sending a specially crafte RPC request, an attacker could overflow th buffer and execute arbitrary ... **Platforms**: win **CVEs**: CVE-2006-5143 **Refs**: source

Metasploit Module	Date	Rank	Details
CA BrightStor Agent for Microsoft SQL Overflow exploit/windows/brightstor/sql_agent	2005-08-02	average	This module exploits a vulnerability in the C BrightStor Agent for Microsoft SQL Server. vulnerability was discovered by cybertronic[at]gmx.net. **Platforms**: win **CVEs**: CVE-2005-1272 **Refs**: source, ref1, ref2
CA BrightStor ARCserve Tape Engine Buffer Overflow exploit/windows/brightstor/tape_engine	2006-11-21	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup r11.1 - r11.5. By sending a speciall crafted DCERPC request, an attacker coul overflow the buffer and ... **Platforms**: win **CVEs**: CVE-2006-6076 **Refs**: source
CA BrightStor ARCserve Tape Engine 0x8A Buffer Overflow exploit/windows/brightstor/tape_engine_0x8a	2010-10-04	average	This module exploits a stack buffer overflo Computer Associates BrightStor ARCserve Backup r11.1 - r11.5. By sending a speciall crafted DCERPC request, an attacker coul overflow the buffer and ... **Platforms**: win **Refs**: source, ref1
CA BrightStor Universal Agent Overflow exploit/windows/brightstor/universal_agent	2005-04-11	average	This module exploits a convoluted heap overflow in the CA BrightStor Universal Ag service. Triple userland exception results ir heap growth and execution of dereference function pointer at a ... **Platforms**: win **CVEs**: CVE-2005-1018 **Refs**: source, ref1
Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow exploit/windows/browser/adobe_cooltype_sing	2010-09-07	great	This module exploits a vulnerability in the S INdependent Glyplets (SING) table handlin within versions 8.2.4 and 9.3.4 of Adobe Reader. Prior versions are assumed to be vulnerable as well. **Platforms**: win **CVEs**: CVE-2010-2883 **Refs**: source, ref1, ref2
Adobe Flash Player AVM Verification Logic Array Indexing Code Execution exploit/windows/browser/adobe_flashplayer_arrayindexing	2012-06-21	great	This module exploits a vulnerability in Adob Flash Player versions 10.3.181.23 and ear This issue is caused by a failure in the ActionScript3 AVM2 verification logic. This results in unsafe ... **Platforms**: win **CVEs**: CVE-2011-2110 **Refs**: source, ref1, ref2, ref3, ref4
Adobe Flash Player AVM Bytecode Verification Vulnerability exploit/windows/browser/adobe_flashplayer_avm	2011-03-15	good	This module exploits a vulnerability in Adob Flash Player versions 10.2.152.33 and ear This issue is caused by a failure in the ActionScript3 AVM2 verification logic. This results in unsafe ... **Platforms**: win **CVEs**: CVE-2011-0609 **Refs**: source, ref1, ref2, ref3, ref4
Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability exploit/windows/browser/adobe_flashplayer_flash10o	2011-04-11	normal	This module exploits a vulnerability in Adob Flash Player that was discovered, and has exploited actively in the wild. By embeddin specially crafted .swf file, Adobe Flash cras due to an ... **Platforms**: win **CVEs**: CVE-2011-0611 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Adobe Flash Player "newfunction" Invalid Pointer Use exploit/windows/browser/adobe_flashplayer_newfunction	2010-06-04	normal	This module exploits a vulnerability in the DoABC tag handling within versions 9.x an 10.0 of Adobe Flash Player. Adobe Reader Acrobat are also vulnerable, as are any oth applications that may ... **Platforms**: win **CVEs**: CVE-2010-1297 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Adobe Flash Player Integer Underflow Remote Code Execution exploit/windows/browser/adobe_flash_avm2	2014-02-05	normal	This module exploits a vulnerability found i ActiveX component of Adobe Flash Player before 12.0.0.43. By supplying a specially crafted swf file it is possible to trigger an in underflow in ... **Platforms**: win **CVEs**: CVE-2014-0497 **Refs**: source, ref1, ref2
Adobe Flash Player casi32 Integer Overflow exploit/windows/browser/adobe_flash_casi32_int_overflow	2014-10-14	great	This module exploits an integer overflow in Adobe Flash Player. The vulnerability occu the casi32 method, where an integer overfl occurs if a ByteArray of length 0 is setup a domainMemory for ... **Platforms**: win **CVEs**: CVE-2014-0569 **Refs**: source, ref1, ref2
Adobe Flash Player copyPixelsToByteArray Method Integer Overflow exploit/windows/browser/adobe_flash_copy_pixels_to_byte_array	2014-09-23	great	This module exploits an integer overflow in Adobe Flash Player. The vulnerability occu the copyPixelsToByteArray method from th BitmapData object. The position field of the destination ... **Platforms**: win **CVEs**: CVE-2014-0556 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Adobe Flash Player domainMemory ByteArray Use After Free exploit/windows/browser/adobe_flash_domain_memory_uaf	2014-04-14	great	This module exploits a use-after-free vulnerability in Adobe Flash Player. The vulnerability occurs when the ByteArray assigned to the current ApplicationDomain freed from an ActionScript worker, ... **Platforms**: win **CVEs**: CVE-2015-0359 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Adobe Flash Player Type Confusion Remote Code Execution exploit/windows/browser/adobe_flash_filters_type_confusion	2013-12-10	normal	This module exploits a type confusion vulnerability found in the ActiveX compone Adobe Flash Player. This vulnerability was found exploited in the wild in November 20 This module has been ... **Platforms**: win **CVEs**: CVE-2013-5331 **Refs**: source, ref1, ref2
Adobe Flash Player MP4 'cprt' Overflow exploit/windows/browser/adobe_flash_mp4_cprt	2012-02-15	normal	This module exploits a vulnerability found i Adobe Flash Player. By supplying a corrup .mp4 file loaded by Flash, it is possible to g arbitrary remote code execution under the context of the ... **Platforms**: win **CVEs**: CVE-2012-0754 **Refs**: source, ref1, ref2
Adobe Flash Player 11.3 Kern Table Parsing Integer Overflow exploit/windows/browser/adobe_flash_otf_font	2012-08-09	normal	This module exploits a vulnerability found i ActiveX component of Adobe Flash Player before 11.3.300.271. By supplying a specia crafted .otf font file with a large nTables val the 'kern' ... **Platforms**: win **CVEs**: CVE-2012-1535 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Adobe Flash Player PCRE Regex Vulnerability exploit/windows/browser/adobe_flash_pcre	2014-11-25	normal	This module exploits a vulnerability found i Adobe Flash Player. A compilation logic er the PCRE engine, specifically in the handli the c escape sequence when followed by a multi-byte ... **Platforms**: win **CVEs**: CVE-2015-0318 **Refs**: source, ref1, ref2
Adobe Flash Player Regular Expression Heap Overflow exploit/windows/browser/adobe_flash_regex_value	2013-02-08	normal	This module exploits a vulnerability found i ActiveX component of Adobe Flash Player before 11.5.502.149. By supplying a specia crafted swf file with special regex value, it i possible to ... **Platforms**: win **CVEs**: CVE-2013-0634 **Refs**: source, ref1, ref2, ref3, ref4, ref5

Metasploit Module	Date	Rank	Details
Adobe Flash Player MP4 SequenceParameterSetNALUnit Buffer Overflow exploit/windows/browser/adobe_flash_sps	2011-08-09	normal	This module exploits a vulnerability found i Adobe Flash Player's Flash10u.ocx compo When processing a MP4 file (specifically th Sequence Parameter Set Flash will see if pic_order_cnt_type is ... **Platforms**: win **CVEs**: CVE-2011-2140 **Refs**: source, ref1, ref2, ref3
Adobe Flash Player UncompressViaZlibVariant Uninitialized Memory exploit/windows/browser/adobe_flash_uncompress_zlib_uninitialized	2014-11-11	good	This module exploits an uninitialized memc vulnerability in Adobe Flash Player. The vulnerability occurs in the ByteArray::UncompressViaZlibVariant metl which fails to initialize allocated ... **Platforms**: win **CVEs**: CVE-2014-8440 **Refs**: source, ref1, ref2, ref3
Adobe Flash Player ByteArray With Workers Use After Free exploit/windows/browser/adobe_flash_worker_byte_array_uaf	2015-02-02	great	This module exploits a use-after-free vulnerability in Adobe Flash Player. The vulnerability occurs when the ByteArray assigned to the current ApplicationDomain freed from an ActionScript worker, ... **Platforms**: win **CVEs**: CVE-2015-0313 **Refs**: source, ref1, ref2, ref3
Adobe FlateDecode Stream Predictor 02 Integer Overflow exploit/windows/browser/adobe_flatedecode_predictor02	2009-10-08	good	This module exploits an integer overflow vulnerability in Adobe Reader and Adobe Acrobat Professional versions before 9.2. **Platforms**: win **CVEs**: CVE-2009-3459 **Refs**: source, ref1, ref2
Adobe Collab.getIcon() Buffer Overflow exploit/windows/browser/adobe_geticon	2009-03-24	good	This module exploits a buffer overflow in A Reader and Adobe Acrobat. Affected versi include < 7.1.1, < 8.1.3, and < 9.1. By crea specially crafted pdf that a contains malfor ... **Platforms**: win **CVEs**: CVE-2009-0927 **Refs**: source, ref1
Adobe JBIG2Decode Heap Corruption exploit/windows/browser/adobe_jbig2decode	2009-02-19	good	This module exploits a heap-based pointer corruption flaw in Adobe Reader 9.0.0 and earlier. This module relies upon javascript f the heap spray. **Platforms**: win **CVEs**: CVE-2009-0658 **Refs**: source, ref1
Adobe Doc.media.newPlayer Use After Free Vulnerability exploit/windows/browser/adobe_media_newplayer	2009-12-14	good	This module exploits a use after free vulnerability in Adobe Reader and Adobe Acrobat Professional versions up to and including 9.2. **Platforms**: win **CVEs**: CVE-2009-4324 **Refs**: source, ref1
Adobe Shockwave rcsL Memory Corruption exploit/windows/browser/adobe_shockwave_rcsl_corruption	2010-10-21	normal	This module exploits a weakness in the Ad Shockwave player's handling of Director m (.DIR). A memory corruption vulnerability o through an undocumented rcsL chunk. **Platforms**: win **CVEs**: CVE-2010-3653 **Refs**: source, ref1
Adobe Reader ToolButton Use After Free exploit/windows/browser/adobe_toolbutton	2013-08-08	normal	This module exploits an use after free conc on Adobe Reader versions 11.0.2, 10.1.6 a 9.5.4 and prior. The vulnerability exists whi handling the ToolButton object, where the cEnable callback ... **Platforms**: win **CVEs**: CVE-2013-3346 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Adobe util.printf() Buffer Overflow exploit/windows/browser/adobe_utilprintf	2008-02-08	good	This module exploits a buffer overflow in A Reader and Adobe Acrobat Professional < 8.1.3. By creating a specially crafted pdf th contains malformed util.printf() entry, an att may be ... **Platforms**: win **CVEs**: CVE-2008-2992 **Refs**: source
Advantech WebAccess dvs.ocx GetColor Buffer Overflow exploit/windows/browser/advantech_webaccess_dvs_getcolor	2014-07-17	normal	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 c reached with user ... **Platforms**: win **CVEs**: CVE-2014-2364 **Refs**: source, ref1
AOL Instant Messenger goaway Overflow exploit/windows/browser/aim_goaway	2004-08-09	great	This module exploits a flaw in the handling AOL Instant Messenger's 'goaway' URI ha An attacker can execute arbitrary code by supplying an overly sized buffer as the 'message' parameter. ... **Platforms**: win **CVEs**: CVE-2004-0636 **Refs**: source, ref1
Aladdin Knowledge System Ltd ChooseFilePath Buffer Overflow exploit/windows/browser/aladdin_choosefilepath_bof	2012-04-01	normal	This module exploits a vulnerability found i Aladdin Knowledge System's ActiveX component. By supplying a long string of d the ChooseFilePath() function, a buffer ove occurs, which may ... **Platforms**: win **Refs**: source
Amaya Browser v11.0 'bdo' Tag Overflow exploit/windows/browser/amaya_bdo	2009-01-28	normal	This module exploits a stack buffer overflo the Amaya v11 Browser. By sending an ov long string to the "bdo" tag, an attacker ma able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2009-0323 **Refs**: source
America Online ICQ ActiveX Control Arbitrary File Download and Execute exploit/windows/browser/aol_icq_downloadagent	2006-11-06	excellent	This module allows remote attackers to download and execute arbitrary files on a u system via the DownloadAgent function of ICQPhone.SipxPhoneManager ActiveX co **Platforms**: win **CVEs**: CVE-2006-5650 **Refs**: source
Apple ITunes 4.7 Playlist Buffer Overflow exploit/windows/browser/apple_itunes_playlist	2005-01-11	normal	This module exploits a stack buffer overflo Apple ITunes 4.7 build 4.7.0.42. By creatin URL link to a malicious PLS file, a remote attacker could overflow a buffer and execu arbitrary code. ... **Platforms**: win **CVEs**: CVE-2005-0043 **Refs**: source
Apple QuickTime 7.6.7 _Marshaled_pUnk Code Execution exploit/windows/browser/apple_quicktime_marshaled_punk	2010-08-30	great	This module exploits a memory trust issue Apple QuickTime 7.6.7. When processing a specially-crafted HTML page, the QuickTim ActiveX control will treat a supplied parame as a trusted pointer. ... **Platforms**: win **CVEs**: CVE-2010-1818 **Refs**: source, ref1
Apple QuickTime 7.7.2 MIME Type Buffer Overflow exploit/windows/browser/apple_quicktime_mime_type	2012-11-07	normal	This module exploits a buffer overflow in A QuickTime 7.7.2. The stack based overflow occurs when processing a malformed Cont Type header. The module has been tested successfully on Safari ... **Platforms**: win **CVEs**: CVE-2012-3753 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Apple Quicktime 7 Invalid Atom Length Buffer Overflow exploit/windows/browser/apple_quicktime_rdrf	2013-05-22	normal	This module exploits a vulnerability found i Apple Quicktime. The flaw is triggered whe Quicktime fails to properly handle the data length for certain atoms such as 'rdrf' or 'dr the Alis ... **Platforms**: win **CVEs**: CVE-2013-1017 **Refs**: source, ref1
Apple QuickTime 7.1.3 RTSP URI Buffer Overflow exploit/windows/browser/apple_quicktime_rtsp	2007-01-01	normal	This module exploits a buffer overflow in A QuickTime 7.1.3. This module was inspirec MOAB-01-01-2007. The Browser target for module was tested against IE 6 and Firefo 1.5.0.3 on Windows ... **Platforms**: win **CVEs**: CVE-2007-0015 **Refs**: source
Apple QuickTime 7.6.6 Invalid SMIL URI Buffer Overflow exploit/windows/browser/apple_quicktime_smil_debug	2010-08-12	good	This module exploits a buffer overflow in A QuickTime 7.6.6. When processing a malfc SMIL uri, a stack-based buffer overflow cai occur when logging an error message. **Platforms**: win **CVEs**: CVE-2010-1799 **Refs**: source, ref1, ref2
Apple QuickTime 7.7.2 TeXML Style Element font-table Field Stack Buffer Overflow exploit/windows/browser/apple_quicktime_texml_font_table	2012-11-07	normal	This module exploits a vulnerability found i Apple QuickTime. When handling a TeXML it is possible to trigger a stack-based buffer overflow, and then gain arbitrary code exec under the ... **Platforms**: win **CVEs**: CVE-2012-3752 **Refs**: source, ref1
Ask.com Toolbar askBar.dll ActiveX Control Buffer Overflow exploit/windows/browser/ask_shortformat	2007-09-24	normal	This module exploits a stack buffer overflo Ask.com Toolbar 4.0.2.53. An attacker may able to execute arbitrary code by sending a overly long string to the "ShortFormat()" me in ... **Platforms**: win **CVEs**: CVE-2007-5107 **Refs**: source
ASUS Net4Switch ipswcom.dll ActiveX Stack Buffer Overflow exploit/windows/browser/asus_net4switch_ipswcom	2012-02-17	normal	This module exploits a vulnerability found i ASUS Net4Switch's ipswcom.dll ActiveX cc A buffer overflow condition is possible in multiple places due to the use of the CxDbgPrint() function, ... **Platforms**: win **CVEs**: CVE-2012-4924 **Refs**: source, ref1
AtHocGov IWSAlerts ActiveX Control Buffer Overflow exploit/windows/browser/athocgov_completeinstallation	2008-02-15	normal	This module exploits a stack buffer overflo AtHocGov IWSAlerts. When sending an ov long string to the CompleteInstallation() me of AtHocGovTBr.dll (6.1.4.36) an attacker r be able to ... **Platforms**: win **Refs**: source
Autodesk IDrop ActiveX Control Heap Memory Corruption exploit/windows/browser/autodesk_idrop	2009-04-02	normal	This module exploits a heap-based memor corruption vulnerability in Autodesk IDrop ActiveX control (IDrop.ocx) version 17.1.51 An attacker can execute arbitrary code by triggering a heap use ... **Platforms**: win **Refs**: source, ref1
SonicWALL Aventail epi.dll AuthCredential Format String exploit/windows/browser/aventail_epi_activex	2010-08-19	normal	This module exploits a format string vulner within version 10.0.4.x and 10.5.1 of the SonicWALL Aventail SSL-VPN Endpoint Interrogator/Installer ActiveX control (epi.dl calling the ... **Platforms**: win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
AwingSoft Winds3D Player SceneURL Buffer Overflow exploit/windows/browser/awingsoft_web3d_bof	2009-07-10	average	This module exploits a data segment buffe overflow within Winds3D Viewer of AwingS Awakening 3.x (WindsPly.ocx v3.6.0.0). Th ActiveX is a plugin of AwingSoft Web3D Pl By setting an overly ... **Platforms**: win **CVEs**: CVE-2009-4588 **Refs**: source, ref1
BaoFeng Storm mps.dll ActiveX OnBeforeVideoDownload Buffer Overflow exploit/windows/browser/baofeng_storm_onbeforevideodownload	2009-04-30	normal	This module exploits a buffer overflow in BaoFeng's Storm media Player ActiveX co Versions of mps.dll including 3.9.4.27 and are affected. When passing an overly long to the method ... **Platforms**: win **CVEs**: CVE-2009-1612 **Refs**: source
RKD Software BarCodeAx.dll v4.9 ActiveX Remote Stack Buffer Overflow exploit/windows/browser/barcode_ax49	2007-06-22	normal	This module exploits a stack buffer overflo RKD Software Barcode Application ActiveX Control 'BarCodeAx.dll'. By sending an ove long string to the BeginPrint method of BarCodeAx.dll v4.9, an ... **Platforms**: win **CVEs**: CVE-2007-3435 **Refs**: source
Black Ice Cover Page ActiveX Control Arbitrary File Download exploit/windows/browser/blackice_downloadimagefileurl	2008-06-05	excellent	This module allows remote attackers to pla arbitrary files on a users file system by abu the "DownloadImageFileURL" method in th Black Ice BIImgFrm.ocx ActiveX Control (BIImgFrm.ocx 12.0.0.0). ... **Platforms**: win **CVEs**: CVE-2008-2683 **Refs**: source
Icona SpA C6 Messenger DownloaderActiveX Control Arbitrary File Download and Execute exploit/windows/browser/c6_messenger_downloaderactivex	2008-06-03	excellent	This module exploits a vulnerability in Icon SpA C6 Messenger 1.0.0.1. The vulnerabil in the DownloaderActiveX Control (DownloaderActiveX.ocx). The insecure co can be abused to download ... **Platforms**: win **CVEs**: CVE-2008-2551 **Refs**: source
CA BrightStor ARCserve Backup AddColumn() ActiveX Buffer Overflow exploit/windows/browser/ca_brightstor_addcolumn	2008-03-16	normal	The CA BrightStor ARCserve Backup Activ control (ListCtrl.ocx) is vulnerable to a stac based buffer overflow. By passing an overl argument to the AddColumn() method, a re attacker could ... **Platforms**: win **CVEs**: CVE-2008-1472 **Refs**: source
Chilkat Crypt ActiveX WriteFile Unsafe Method exploit/windows/browser/chilkat_crypt_writefile	2008-11-03	excellent	This module allows attackers to execute co via the 'WriteFile' unsafe method of Chilkat Software Inc's Crypt ActiveX control. This exploit is based on shinnai's exploit that us hcp:// protocol ... **Platforms**: win **CVEs**: CVE-2008-5002 **Refs**: source
Chrome 72.0.3626.119 FileReader UaF exploit for Windows 7 x86 exploit/windows/browser/chrome_filereader_uaf	2019-03-21	manual	This exploit takes advantage of a use after vulnerability in Google Chrome 72.0.3626. running on Windows 7 x86. The FileReader.readAsArrayBuffer function can return multiple references to the ... **Platforms**: win **CVEs**: CVE-2019-5786 **Refs**: source, ref1, ref2, ref3, ref4
Cisco AnyConnect VPN Client ActiveX URL Property Download and Execute exploit/windows/browser/cisco_anyconnect_exec	2011-06-01	excellent	This module exploits a vulnerability in the C AnyConnect VPN client vpnweb.ocx Active control. This control is typically used to inst the VPN client. An attacker can set the 'url' property ... **Platforms**: win **CVEs**: CVE-2011-2039 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Cisco Linksys PlayerPT ActiveX Control Buffer Overflow exploit/windows/browser/cisco_playerpt_setsource	2012-03-22	normal	This module exploits a vulnerability found i Cisco Linksys PlayerPT 1.0.0.15 as the ins with the web interface of Cisco Linksys WVC200 Wireless-G PTZ Internet Video Camera. The vulnerability, ... **Platforms**: win **CVEs**: CVE-2012-0284 **Refs**: source
Cisco Linksys PlayerPT ActiveX Control SetSource sURL Argument Buffer Overflow exploit/windows/browser/cisco_playerpt_setsource_surl	2012-07-17	normal	This module exploits a vulnerability found i Cisco Linksys PlayerPT 1.0.0.15 as the ins with the web interface of Cisco Linksys WVC200 Wireless-G PTZ Internet Video Camera. The vulnerability, ... **Platforms**: win **CVEs**: CVE-2012-0284 **Refs**: source, ref1
Cisco WebEx Chrome Extension RCE (CVE-2017-3823) exploit/windows/browser/cisco_webex_ext	2017-01-21	great	This module exploits a vulnerability presen the Cisco WebEx Chrome Extension versi 1.0.1 which allows an attacker to execute arbitrary commands on a system. **Platforms**: win **CVEs**: CVE-2017-3823 **Refs**: source
Citrix Gateway ActiveX Control Stack Based Buffer Overflow Vulnerability exploit/windows/browser/citrix_gateway_actx	2011-07-14	normal	This module exploits a stack based buffer overflow in the Citrix Gateway ActiveX con Exploitation of this vulnerability requires us interaction. The victim must click a button i dialog to ... **Platforms**: win **CVEs**: CVE-2011-2882 **Refs**: source, ref1
IBM Rational ClearQuest CQOle Remote Code Execution exploit/windows/browser/clear_quest_cqole	2012-05-19	normal	This module exploits a function prototype mismatch on the CQOle ActiveX control in 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 ... **Platforms**: win **CVEs**: CVE-2012-0708 **Refs**: source, ref1, ref2
CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow exploit/windows/browser/communicrypt_mail_activex	2010-05-19	great	This module exploits a stack buffer overflo the ANSMTP.dll/AOSMTP.dll ActiveX Contr provided by CommuniCrypt Mail 1.16. By sending an overly long string to the "AddAttachments()" method, an ... **Platforms**: win **Refs**: source
Adobe Flash Player Object Type Confusion exploit/windows/browser/adobe_flash_rtmp	2012-05-04	normal	This module exploits a vulnerability found i Adobe Flash Player. By supplying a corrup AMF0 "_error" response, it is possible to ga arbitrary remote code execution under the context of the user. ... **Platforms**: win **CVEs**: CVE-2012-0779 **Refs**: source, ref1, ref2, ref3
AOL Radio AmpX ActiveX Control ConvertFile() Buffer Overflow exploit/windows/browser/aol_ampx_convertfile	2009-05-19	normal	This module exploits a stack-based buffer overflow in AOL IWinAmpActiveX class (AmpX.dll) version 2.4.0.6 installed via AO Radio website. By setting an overly long va to 'ConvertFile()', an ... **Platforms**: win **Refs**: source
AwingSoft Winds3D Player 3.5 SceneURL Download and Execute exploit/windows/browser/awingsoft_winds3d_sceneurl	2009-11-14	excellent	This module exploits an untrusted program execution vulnerability within the Winds3D Player from AwingSoft. The Winds3D Play browser plugin for IE (ActiveX), Opera (DL and Firefox (XPI). By ... **Platforms**: win **CVEs**: CVE-2009-4850 **Refs**: source

Metasploit Module	Date	Rank	Details
Creative Software AutoUpdate Engine ActiveX Control Buffer Overflow exploit/windows/browser/creative_software_cachefolder	2008-05-28	normal	This module exploits a stack buffer overflo Creative Software AutoUpdate Engine. Wh sending an overly long string to the cachefolder() property of CTSUEng.ocx an attacker may be able to execute ... **Platforms**: win **CVEs**: CVE-2008-0955 **Refs**: source
Green Dam URL Processing Buffer Overflow exploit/windows/browser/greendam_url	2009-06-11	normal	This module exploits a stack-based buffer overflow in Green Dam Youth Escort versic 3.17 in the way it handles overly long URLs setting an overly long URL, an attacker car overrun a buffer and ... **Platforms**: win **Refs**: source, ref1, ref2
IBM Tivoli Provisioning Manager Express for Software Distribution Isig.isigCtl.1 ActiveX RunAndUploadFile() Method Overflow exploit/windows/browser/ibm_tivoli_pme_activex_bof	2012-03-01	normal	This module exploits a buffer overflow vulnerability in the Isig.isigCtl.1 ActiveX ins with IBM Tivoli Provisioning Manager Expr for Software Distribution 4.1.1. The vulnera is found ... **Platforms**: win **CVEs**: CVE-2012-0198 **Refs**: source
Java MixerSequencer Object GM_Song Structure Handling Vulnerability exploit/windows/browser/java_mixer_sequencer	2010-03-30	great	This module exploits a flaw within the hanc of MixerSequencer objects in Java 6u18 ar before. Exploitation id done by supplying a specially crafted MIDI file within an RMF Fi When the ... **Platforms**: win **CVEs**: CVE-2010-0842 **Refs**: source, ref1
McAfee Virtual Technician MVTControl 6.3.0.1911 GetObject Vulnerability exploit/windows/browser/mcafee_mvt_exec	2012-04-30	excellent	This module exploits a vulnerability found i McAfee Virtual Technician's MVTControl. T ActiveX control can be abused by using the GetObject() function to load additional unsa classes such as ... **Platforms**: win **CVEs**: CVE-2012-4598 **Refs**: source, ref1
MS06-057 Microsoft Internet Explorer WebViewFolderIcon setSlice() Overflow exploit/windows/browser/ms06_057_webview_setslice	2006-07-17	normal	This module exploits a flaw in the WebViewFolderIcon ActiveX control includ with Windows 2000, Windows XP, and Win 2003. This flaw was published during the M of Browser Bugs project (MoBB ... **Platforms**: win **CVEs**: CVE-2006-3730 **Refs**: source
MS10-018 Microsoft Internet Explorer Tabular Data Control ActiveX Memory Corruption exploit/windows/browser/ms10_018_ie_tabular_activex	2010-03-09	good	This module exploits a memory corruption vulnerability in the Internet Explorer Tabula Data ActiveX Control. Microsoft reports tha version 5.01 and 6 of Internet Explorer are vulnerable. By ... **Platforms**: win **CVEs**: CVE-2010-0805 **Refs**: source
MS13-037 Microsoft Internet Explorer COALineDashStyleArray Integer Overflow exploit/windows/browser/ms13_037_svg_dashstyle	2013-03-06	normal	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 th vgx.dll module. The exploit ... **Platforms**: win **CVEs**: CVE-2013-2551 **Refs**: source, ref1
Symantec Norton Internet Security 2004 ActiveX Control Buffer Overflow exploit/windows/browser/nis2004_get	2007-05-16	normal	This module exploits a stack buffer overflo the ISAlertDataCOM ActiveX Control (ISLAert.dll) provided by Symantec Norton Internet Security 2004. By sending an over long string to the "Get()" ... **Platforms**: win **CVEs**: CVE-2007-1689 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Orbit Downloader Connecting Log Creation Buffer Overflow exploit/windows/browser/orbit_connecting	2009-02-03	normal	This module exploits a stack buffer overflo Orbit Downloader 2.8.4. When an attacker serves up a malicious web site, arbitrary co may be executed. The PAYLOAD windows/shell_bind_tcp works best. **Platforms**: win **CVEs**: CVE-2009-0187 **Refs**: source
SAP AG SAPgui EAI WebViewer3D Buffer Overflow exploit/windows/browser/sapgui_saveviewtosessionfile	2009-03-31	normal	This module exploits a stack buffer overflo Siemens Unigraphics Solutions Teamcente Visualization EAI WebViewer3D ActiveX co that is bundled with SAPgui. When passing overly long string ... **Platforms**: win **CVEs**: CVE-2007-4475 **Refs**: source
Tumbleweed FileTransfer vcst_eu.dll ActiveX Control Buffer Overflow exploit/windows/browser/tumbleweed_filetransfer	2008-04-07	great	This module exploits a stack buffer overflo the vcst_eu.dll FileTransfer Module (1.0.0.5 ActiveX control in the Tumbleweed SecureTransport suite. By sending an over long string to the ... **Platforms**: win **CVEs**: CVE-2008-1724 **Refs**: source, ref1
Crystal Reports CrystalPrintControl ActiveX ServerResourceVersion Property Overflow exploit/windows/browser/crystal_reports_printcontrol	2010-12-14	normal	This module exploits a heap based buffer overflow in the CrystalPrintControl ActiveX while handling the ServerResourceVersion property. The affected control can be found the PrintControl.dll ... **Platforms**: win **CVEs**: CVE-2010-2590 **Refs**: source
Dell Webcam CrazyTalk ActiveX BackImage Vulnerability exploit/windows/browser/dell_webcam_crazytalk	2012-03-19	normal	This module exploits a vulnerability in Dell Webcam's CrazyTalk component. Specifica when supplying a long string for a file path the BackImage property, an overflow may o after checking ... **Platforms**: win **Refs**: source, ref1
Worldweaver DX Studio Player shell.execute() Command Execution exploit/windows/browser/dxstudio_player_exec	2009-06-09	excellent	This module exploits a command execution vulnerability within the DX Studio Player fro Worldweaver for versions 3.0.29 and earlie The player is a browser plugin for IE (Activ and Firefox (dll). ... **Platforms**: win **CVEs**: CVE-2009-2011 **Refs**: source, ref1
Electronic Arts SnoopyCtrl ActiveX Control Buffer Overflow exploit/windows/browser/ea_checkrequirements	2007-10-08	normal	This module exploits a stack buffer overflo Electronic Arts SnoopyCtrl ActiveX Control (NPSnpy.dll 1.1.0.36. When sending an ov long string to the CheckRequirements() me an attacker may ... **Platforms**: win **CVEs**: CVE-2007-4466 **Refs**: source
FlipViewer FViewerLoading ActiveX Control Buffer Overflow exploit/windows/browser/ebook_flipviewer_fviewerloading	2007-06-06	normal	This module exploits a stack buffer overflo E-BOOK Systems FlipViewer 4.0. The vulnerability is caused due to a boundary e in the FViewerLoading (FlipViewerX.dll) Ac control when ... **Platforms**: win **CVEs**: CVE-2007-2919 **Refs**: source
EnjoySAP SAP GUI ActiveX Control Arbitrary File Download exploit/windows/browser/enjoysapgui_comp_download	2009-04-15	excellent	This module allows remote attackers to pla arbitrary files on a users file system by abu the "Comp_Download" method in the SAP KWEdit ActiveX Control (kwedit.dll 6400.1. **Platforms**: win **CVEs**: CVE-2008-4830 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
EnjoySAP SAP GUI ActiveX Control Buffer Overflow exploit/windows/browser/enjoysapgui_preparetoposthtml	2007-07-05	normal	This module exploits a stack buffer overflo SAP KWEdit ActiveX Control (kwedit.dll 6400.1.1.41) provided by EnjoySAP GUI. E sending an overly long string to the "PrepareToPostHTML()" method, an ... **Platforms**: win **CVEs**: CVE-2007-3605 **Refs**: source
Exodus Wallet (ElectronJS Framework) remote Code Execution exploit/windows/browser/exodus	2018-01-25	manual	This module exploits a Remote Code Exec vulnerability in Exodus Wallet, a vulnerabili the ElectronJS Framework protocol handle be used to get arbitrary command executio the user ... **Platforms**: win **CVEs**: CVE-2018-1000006 **Refs**: source
Facebook Photo Uploader 4 ActiveX Control Buffer Overflow exploit/windows/browser/facebook_extractiptc	2008-01-31	normal	This module exploits a stack buffer overflo Facebook Photo Uploader 4. By sending a overly long string to the "ExtractIptc()" prop located in the ImageUploader4.ocx (4.5.57 Control, an ... **Platforms**: win **CVEs**: CVE-2008-5711 **Refs**: source
Firefox nsSMILTimeContainer::NotifyTimeChange() RCE exploit/windows/browser/firefox_smil_uaf	2016-11-30	normal	This module exploits an out-of-bounds indexing/use-after-free condition present in nsSMILTimeContainer::NotifyTimeChange(across numerous versions of Mozilla Firefo Microsoft Windows. **Platforms**: win **CVEs**: CVE-2016-9079 **Refs**: source, ref1, ref2
Foxit Reader Plugin URL Processing Buffer Overflow exploit/windows/browser/foxit_reader_plugin_url_bof	2013-01-07	normal	This module exploits a vulnerability in the F Reader Plugin, it exists in the npFoxitReaderPlugin.dll module. When loa PDF files from remote hosts, overly long qu strings within URLs can ... **Platforms**: win **Refs**: source, ref1
GetGo Download Manager HTTP Response Buffer Overflow exploit/windows/browser/getgodm_http_response_bof	2014-03-09	normal	This module exploits a stack-based buffer overflow vulnerability in GetGo Download Manager version 5.3.0.2712 earlier, caused an overly long HTTP response header. By persuading the victim to ... **Platforms**: win **CVEs**: CVE-2014-2206 **Refs**: source
GOM Player ActiveX Control Buffer Overflow exploit/windows/browser/gom_openurl	2007-10-27	normal	This module exploits a stack buffer overflo GOM Player 2.1.6.3499. By sending an ov long string to the "OpenUrl()" method locat the GomWeb3.dll Control, an attacker may able to ... **Platforms**: win **CVEs**: CVE-2007-5779 **Refs**: source, ref1
Honeywell HSC Remote Deployer ActiveX Remote Code Execution exploit/windows/browser/honeywell_hscremotedeploy_exec	2013-02-22	excellent	This module exploits a vulnerability found i Honeywell HSC Remote Deployer ActiveX control can be abused by using the LaunchInstaller() function to execute an arbitrary HTA from a remote ... **Platforms**: win **CVEs**: CVE-2013-0108 **Refs**: source, ref1, ref2
Honeywell Tema Remote Installer ActiveX Remote Code Execution exploit/windows/browser/honeywell_tema_exec	2011-10-20	excellent	This module exploits a vulnerability found i Honeywell Tema ActiveX Remote Installer. ActiveX control can be abused by using the DownloadFromURL() function to install an arbitrary MSI from ... **Platforms**: win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
HP Mercury Quality Center ActiveX Control ProgColor Buffer Overflow exploit/windows/browser/hpmqc_progcolor	2007-04-04	normal	This module exploits a stack-based buffer overflow in SPIDERLib.Loader ActiveX cor (Spider90.ocx) 9.1.0.4353 installed by TestDirector (TD) for Hewlett-Packard Mer Quality Center 9.0 before ... **Platforms**: win **CVEs**: CVE-2007-1819 **Refs**: source, ref1
HP Application Lifecycle Management XGO.ocx ActiveX SetShapeNodeType() Remote Code Execution exploit/windows/browser/hp_alm_xgo_setshapenodetype_exec	2012-08-29	normal	This module exploits a vulnerability within t XGO.ocx ActiveX Control installed with the Application Lifecycle Manager Client. The vulnerability exists in the SetShapeNodeTy method, which ... **Platforms**: win **Refs**: source
HP Easy Printer Care XMLCacheMgr Class ActiveX Control Remote Code Execution exploit/windows/browser/hp_easy_printer_care_xmlcachemgr	2012-01-11	great	This module allows remote attackers to pla arbitrary files on a users file system by abu the "CacheDocumentXMLWithId" method f the "XMLCacheMgr" class in the HP Easy Printer HPTicketMgr.dll ... **Platforms**: win **CVEs**: CVE-2011-4786 **Refs**: source
HP Easy Printer Care XMLSimpleAccessor Class ActiveX Control Remote Code Execution exploit/windows/browser/hp_easy_printer_care_xmlsimpleaccessor	2011-08-16	great	This module allows remote attackers to pla arbitrary files on a users file system by abu via Directory Traversal attack the "saveXM method from the "XMLSimpleAccessor" cla the HP Easy ... **Platforms**: win **CVEs**: CVE-2011-2404 **Refs**: source
Persits XUpload ActiveX AddFile Buffer Overflow exploit/windows/browser/hp_loadrunner_addfile	2008-01-25	normal	This module exploits a stack buffer overflo Persits Software Inc's XUpload ActiveX control(version 3.0.0.3) thats included in H LoadRunner 9.5. By passing an overly long string to the AddFile ... **Platforms**: win **CVEs**: CVE-2008-0492 **Refs**: source
HP LoadRunner 9.0 ActiveX AddFolder Buffer Overflow exploit/windows/browser/hp_loadrunner_addfolder	2007-12-25	good	This module exploits a stack buffer overflo Persits Software Inc's XUpload ActiveX control(version 2.1.0.1) thats included in H LoadRunner 9.0. By passing an overly long string to the AddFolder ... **Platforms**: win **CVEs**: CVE-2007-6530 **Refs**: source
HP LoadRunner lrFileIOService ActiveX Remote Code Execution exploit/windows/browser/hp_loadrunner_writefilebinary	2013-07-24	normal	This module exploits a vulnerability on the lrFileIOService ActiveX, as installed with H LoadRunner 11.50. The vulnerability exists the WriteFileBinary method where user pro data is used as ... **Platforms**: win **CVEs**: CVE-2013-2370 **Refs**: source, ref1
HP LoadRunner lrFileIOService ActiveX WriteFileString Remote Code Execution exploit/windows/browser/hp_loadrunner_writefilestring	2013-07-24	normal	This module exploits a vulnerability on the lrFileIOService ActiveX, as installed with H LoadRunner 11.50. The vulnerability exists the WriteFileString method, which allow the to write ... **Platforms**: win **CVEs**: CVE-2013-4798 **Refs**: source, ref1
Hyleos ChemView ActiveX Control Stack Buffer Overflow exploit/windows/browser/hyleos_chemviewx_activex	2010-02-10	good	This module exploits a stack-based buffer overflow within version 1.9.5.1 of Hyleos ChemView (HyleosChemView.ocx). By call the 'SaveAsMolFile' or 'ReadMolFile' meth with an overly long first ... **Platforms**: win **CVEs**: CVE-2010-0679 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
IBM Access Support ActiveX Control Buffer Overflow exploit/windows/browser/ibmegath_getxmlvalue	2009-03-24	normal	This module exploits a stack buffer overflo IBM Access Support. When sending an ov long string to the GetXMLValue() method o IbmEgath.dll (3.20.284.0) an attacker may able to execute ... **Platforms**: win **CVEs**: CVE-2009-0215 **Refs**: source
IBM Lotus Domino Web Access Upload Module Buffer Overflow exploit/windows/browser/ibmlotusdomino_dwa_uploadmodule	2007-12-20	normal	This module exploits a stack buffer overflo IBM Lotus Domino Web Access Upload M By sending an overly long string to the "General_ServerName()" property located dwa7w.dll and the ... **Platforms**: win **CVEs**: CVE-2007-4474 **Refs**: source
IBM SPSS SamplePower C1Tab ActiveX Heap Overflow exploit/windows/browser/ibm_spss_c1sizer	2013-04-26	normal	This module exploits a heap based buffer overflow in the C1Tab ActiveX control, whil handling the TabCaption property. The affe control can be found in the c1sizer.ocx component as included with ... **Platforms**: win **CVEs**: CVE-2012-5946 **Refs**: source, ref1
MS13-008 Microsoft Internet Explorer CButton Object Use-After-Free Vulnerability exploit/windows/browser/ie_cbutton_uaf	2012-12-27	normal	This module exploits a vulnerability found i Microsoft Internet Explorer. A use-after-free condition occurs when a CButton object is but a reference is kept and used again dur page ... **Platforms**: win **CVEs**: CVE-2012-4792 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref
MS13-038 Microsoft Internet Explorer CGenericElement Object Use-After-Free Vulnerability exploit/windows/browser/ie_cgenericelement_uaf	2013-05-03	good	This module exploits a vulnerability found i Microsoft Internet Explorer. A use-after-free condition occurs when a CGenericElement object is freed, but a reference is kept on th Document and used ... **Platforms**: win **CVEs**: CVE-2013-1347 **Refs**: source, ref1, ref2
MS06-014 Microsoft Internet Explorer COM CreateObject Code Execution exploit/windows/browser/ie_createobject	2006-04-11	excellent	This module exploits a generic code execu vulnerability in Internet Explorer by abusing vulnerable ActiveX objects. **Platforms**: win **CVEs**: CVE-2006-0003, CVE-2006-4704 **Refs**: source
MS12-063 Microsoft Internet Explorer execCommand Use-After-Free Vulnerability exploit/windows/browser/ie_execcommand_uaf	2012-09-14	good	This module exploits a vulnerability found i Microsoft Internet Explorer (MSIE). When rendering an HTML page, the CMshtmlEd object gets deleted in an unexpected manr but the same memory is reused ... **Platforms**: win **CVEs**: CVE-2012-4969 **Refs**: source, ref1, ref2
Microsoft Internet Explorer isComponentInstalled Overflow exploit/windows/browser/ie_iscomponentinstalled	2006-02-24	normal	This module exploits a stack buffer overflo Internet Explorer. This bug was patched in Windows 2000 SP4 and Windows XP SP1 according to MSRC. **Platforms**: win **CVEs**: CVE-2006-1016 **Refs**: source
MS13-080 Microsoft Internet Explorer SetMouseCapture Use-After-Free exploit/windows/browser/ie_setmousecapture_uaf	2013-09-17	normal	This module exploits a use-after-free vulnerability that currents targets Internet Explorer 9 on Windows 7, but the flaw shou exist in versions 6/7/8/9/10/11. It was initial found in the wild in ... **Platforms**: win **CVEs**: CVE-2013-3893 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Microsoft Internet Explorer Unsafe Scripting Misconfiguration exploit/windows/browser/ie_unsafe_scripting	2010-09-20	manual	This exploit takes advantage of the "Initializ and script ActiveX controls not marked safe scripting" setting within Internet Explorer. W this option is set, IE allows access to the .. **Platforms**: win **Refs**: source, ref1, ref2, ref3
Viscom Image Viewer CP Pro 8.0/Gold 6.0 ActiveX Control exploit/windows/browser/imgeviewer_tifmergemultifiles	2010-03-03	normal	This module exploits a stack based buffer overflow in the Active control file ImageViewer2.OCX by passing an overly l argument to an insecure TifMergeMultiFiles method. Exploitation results in ... **Platforms**: win **CVEs**: CVE-2010-5193 **Refs**: source, ref1, ref2
InduSoft Web Studio ISSymbol.ocx InternationalSeparator() Heap Overflow exploit/windows/browser/indusoft_issymbol_internationalseparator	2012-04-28	normal	This module exploits a heap overflow found InduSoft Web Studio <= 61.6.00.00 SP6. T overflow exists in the ISSymbol.ocx, and ca triggered with a long string argument for th **Platforms**: win **CVEs**: CVE-2011-0340 **Refs**: source, ref1
IBM Lotus iNotes dwa85W ActiveX Buffer Overflow exploit/windows/browser/inotes_dwa85w_bof	2012-06-01	normal	This module exploits a buffer overflow vulnerability on the UploadControl ActiveX. vulnerability exists in the handling of the "Attachment_Times" property, due to the insecure usage of the ... **Platforms**: win **CVEs**: CVE-2012-2175 **Refs**: source, ref1
Quest InTrust Annotation Objects Uninitialized Pointer exploit/windows/browser/intrust_annotatex_add	2012-03-28	average	This module exploits an uninitialized variab vulnerability in the Annotation Objects Activ component. The ActiveX component loads memory without opting into ALSR so this module exploits the ... **Platforms**: win **CVEs**: CVE-2012-5896 **Refs**: source
Sun Java Web Start BasicServiceImpl Code Execution exploit/windows/browser/java_basicservice_impl	2010-10-12	excellent	This module exploits a vulnerability in Java Runtime Environment that allows an attack escape the Java Sandbox. By injecting a parameter into a javaws call within the BasicServiceImpl class the ... **Platforms**: java, win **CVEs**: CVE-2010-3563 **Refs**: source, ref1
Java CMM Remote Code Execution exploit/windows/browser/java_cmm	2013-03-01	normal	This module abuses the Color Managemer classes from a Java Applet to run arbitrary code outside of the sandbox as exploited in wild in February and March of 2013. The vulnerability affects ... **Platforms**: java, win **CVEs**: CVE-2013-1493 **Refs**: source, ref1, ref2, ref3
Sun Java Applet2ClassLoader Remote Code Execution exploit/windows/browser/java_codebase_trust	2011-02-15	excellent	This module exploits a vulnerability in the J Runtime Environment that allows an attack run an applet outside of the Java Sandbox When an applet is invoked with: 1. A "codebase" parameter ... **Platforms**: java, win **CVEs**: CVE-2010-4452 **Refs**: source, ref1, ref2
Sun Java Runtime New Plugin docbase Buffer Overflow exploit/windows/browser/java_docbase_bof	2010-10-12	great	This module exploits a flaw in the new plug component of the Sun Java Runtime Environment before v6 Update 22. By spec specific parameters to the new plugin, an attacker can cause a ... **Platforms**: win **CVEs**: CVE-2010-3552 **Refs**: source, ref1, ref2, ref3, ref4

Metasploit Module	Date	Rank	Details
Sun Java Web Start Plugin Command Line Argument Injection exploit/windows/browser/java_ws_arginject_altjvm	2010-04-09	excellent	This module exploits a flaw in the Web Sta plugin component of Sun Java Web Start. arguments passed to Java Web Start are r properly validated. By passing the lesser k -J option, an ... **Platforms**: win **CVEs**: CVE-2010-0886, CVE-2010-1423 **Refs**: source, ref1, ref2
Sun Java Web Start Double Quote Injection exploit/windows/browser/java_ws_double_quote	2012-10-16	excellent	This module exploits a flaw in the Web Sta component of the Sun Java Runtime Environment. Parameters initial-heap-size max-heap-size in a JNLP file can contain a double quote which is not ... **Platforms**: win **CVEs**: CVE-2012-0500, CVE-2012-1533 **Refs**: source, ref1, ref2
Sun Java Web Start Plugin Command Line Argument Injection exploit/windows/browser/java_ws_vmargs	2012-02-14	excellent	This module exploits a flaw in the Web Sta component of the Sun Java Runtime Environment. The arguments passed to Ja Web Start are not properly validated, allow injection of arbitrary ... **Platforms**: win **CVEs**: CVE-2012-0500 **Refs**: source, ref1, ref2
Juniper SSL-VPN IVE JuniperSetupDLL.dll ActiveX Control Buffer Overflow exploit/windows/browser/juniper_sslvpn_ive_setupdll	2006-04-26	normal	This module exploits a stack buffer overflo the JuniperSetupDLL.dll library which is ca by the JuniperSetup.ocx ActiveX control, a of the Juniper SSL-VPN (IVE) appliance. B specifying ... **Platforms**: win **CVEs**: CVE-2006-2086 **Refs**: source, ref1
Kazaa Altnet Download Manager ActiveX Control Buffer Overflow exploit/windows/browser/kazaa_altnet_heap	2007-10-03	normal	This module exploits a stack buffer overflo the Altnet Download Manager ActiveX Con (amd4.dll) bundled with Kazaa Media Desk 3.2.7. By sending an overly long string to th "Install()" ... **Platforms**: win **CVEs**: CVE-2007-5217 **Refs**: source, ref1
KeyHelp ActiveX LaunchTriPane Remote Code Execution Vulnerability exploit/windows/browser/keyhelp_launchtripane_exec	2012-06-26	excellent	This module exploits a code execution vulnerability in the KeyScript ActiveX contr from keyhelp.ocx. It is packaged in several products or GE, such as Proficy Historian 4 4.0, 3.5, and 3.1, ... **Platforms**: win **CVEs**: CVE-2012-2516 **Refs**: source, ref1
Logitech VideoCall ActiveX Control Buffer Overflow exploit/windows/browser/logitechvideocall_start	2007-05-31	normal	This module exploits a stack buffer overflo the Logitech VideoCall ActiveX Control (wcamxmp.dll 2.0.3470.448). By sending a overly long string to the "Start()" method, a attacker may be able to ... **Platforms**: win **CVEs**: CVE-2007-2918 **Refs**: source
iseemedia / Roxio / MGI Software LPViewer ActiveX Control Buffer Overflow exploit/windows/browser/lpviewer_url	2008-10-06	normal	This module exploits a stack buffer overflo LPViewer ActiveX control (LPControlI.dll 3.2.0.2). When sending an overly long strir the URL() property an attacker may be abl execute ... **Platforms**: win **CVEs**: CVE-2008-4384 **Refs**: source
Macrovision InstallShield Update Service Buffer Overflow exploit/windows/browser/macrovision_downloadandexecute	2007-10-31	normal	This module exploits a stack buffer overflo Macrovision InstallShield Update Service(Isusweb.dll 6.0.100.54472). By pa an overly long ProductCode string to the DownloadAndExecute method, an ... **Platforms**: win **CVEs**: CVE-2007-5660 **Refs**: source

Metasploit Module	Date	Rank	Details
Macrovision InstallShield Update Service ActiveX Unsafe Method exploit/windows/browser/macrovision_unsafe	2007-10-20	excellent	This module allows attackers to execute cc via an unsafe method in Macrovision InstallShield 2008. **Platforms**: win **CVEs**: CVE-2007-5660 **Refs**: source
Malwarebytes Anti-Malware and Anti-Exploit Update Remote Code Execution exploit/windows/browser/malwarebytes_update_exec	2014-12-16	good	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 ... **Platforms**: win **CVEs**: CVE-2014-4936 **Refs**: source, ref1
Maxthon3 about:history XCS Trusted Zone Code Execution exploit/windows/browser/maxthon_history_xcs	2012-11-26	excellent	Cross Context Scripting (XCS) is possible Maxthon about:history page. Injection in su privileged/trusted browser zone can be use modify configuration settings and execute arbitrary ... **Platforms**: win **Refs**: source, ref1
McAfee Visual Trace ActiveX Control Buffer Overflow exploit/windows/browser/mcafeevisualtrace_tracetarget	2007-07-07	normal	This module exploits a stack buffer overflo the McAfee Visual Trace 3.25 ActiveX Con (NeoTraceExplorer.dll 1.0.0.1). By sending overly long string to the "TraceTarget()" me an ... **Platforms**: win **CVEs**: CVE-2006-6707 **Refs**: source, ref1
McAfee Subscription Manager Stack Buffer Overflow exploit/windows/browser/mcafee_mcsubmgr_vsprintf	2006-08-01	normal	This module exploits a flaw in the McAfee Subscription Manager ActiveX control. Due an unsafe use of vsprintf, it is possible to tr a stack buffer overflow by passing a large s to one of ... **Platforms**: win **CVEs**: CVE-2006-3961 **Refs**: source
mIRC IRC URL Buffer Overflow exploit/windows/browser/mirc_irc_url	2003-10-13	normal	This module exploits a stack buffer overflo mIRC 6.1. By submitting an overly long and specially crafted URL to the 'irc' protocol, a attacker can overwrite the buffer and contr program ... **Platforms**: win **CVEs**: CVE-2003-1336 **Refs**: source
Firefox 8/9 AttributeChildRemoved() Use-After-Free exploit/windows/browser/mozilla_attribchildremoved	2011-12-06	average	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 stil accessible after removal due to a ... **Platforms**: win **CVEs**: CVE-2011-3659 **Refs**: source, ref1
Firefox onreadystatechange Event DocumentViewerImpl Use After Free exploit/windows/browser/mozilla_firefox_onreadystatechange	2013-06-25	normal	This module exploits a vulnerability found c Firefox 17.0.6, specifically a use after free DocumentViewerImpl object, triggered via specially crafted web page using onreadystatechange events ... **Platforms**: win **CVEs**: CVE-2013-1690 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Firefox XMLSerializer Use After Free exploit/windows/browser/mozilla_firefox_xmlserializer	2013-01-08	normal	This module exploits a vulnerability found c Firefox 17.0 (< 17.0.2), specifically a use-a free of an Element object, when using the serializeToStream method with a specially crafted ... **Platforms**: win **CVEs**: CVE-2013-0753 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Mozilla Firefox Interleaved document.write/appendChild Memory Corruption exploit/windows/browser/mozilla_interleaved_write	2010-10-25	normal	This module exploits a code execution vulnerability in Mozilla Firefox caused by interleaved calls to document.write and appendChild. This module was written bas a live exploit found in the wild. **Platforms**: win **CVEs**: CVE-2010-3765 **Refs**: source, ref1, ref2
Mozilla Firefox 3.6.16 mChannel Use-After-Free Vulnerability exploit/windows/browser/mozilla_mchannel	2011-05-10	normal	This module exploits a use after free vulnerability in Mozilla Firefox 3.6.16. An OBJECT Element mChannel can be freed the OnChannelRedirect method of the nsIChannelEventSink Interface. mChannel **Platforms**: win **CVEs**: CVE-2011-0065 **Refs**: source, ref1, ref2
Firefox nsSVGValue Out-of-Bounds Access Vulnerability exploit/windows/browser/mozilla_nssvgvalue	2011-12-06	average	This module exploits an out-of-bounds acc flaw in Firefox 7 and 8 (<= 8.0.1). The notification of nsSVGValue observers via nsSVGValue::NotifyObservers(x,y) uses a which can result in an ... **Platforms**: win **CVEs**: CVE-2011-3658 **Refs**: source, ref1
Mozilla Firefox "nsTreeRange" Dangling Pointer Vulnerability exploit/windows/browser/mozilla_nstreerange	2011-02-02	normal	This module exploits a code execution vulnerability in Mozilla Firefox 3.6.x <= 3.6. and 3.5.x <= 3.5.17 found in nsTreeSelecti By overwriting a subfunction of invalidateSelection it is possible ... **Platforms**: win **CVEs**: CVE-2011-0073 **Refs**: source, ref1, ref2
Mozilla Firefox Array.reduceRight() Integer Overflow exploit/windows/browser/mozilla_reduceright	2011-06-21	normal	This module exploits a vulnerability found i Mozilla Firefox 3.6. When an array object is configured with a large length value, the reduceRight() method may cause an invali index being used, ... **Platforms**: win **CVEs**: CVE-2011-2371 **Refs**: source, ref1
MS03-020 Microsoft Internet Explorer Object Type exploit/windows/browser/ms03_020_ie_objecttype	2003-06-04	normal	This module exploits a vulnerability in Inter Explorer's handling of the OBJECT type attribute. **Platforms**: win **CVEs**: CVE-2003-0344 **Refs**: source
MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution exploit/windows/browser/ms05_054_onload	2005-11-21	normal	This bug is triggered when the browser har a JavaScript 'onLoad' handler in conjunctio with an improperly initialized 'window()' JavaScript function. This exploit results in a to an address ... **Platforms**: win **CVEs**: CVE-2005-1790 **Refs**: source
Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution exploit/windows/browser/ms06_001_wmf_setabortproc	2005-12-27	great	This module exploits a vulnerability in the G library included with Windows XP and 2003 This vulnerability uses the 'Escape' metafil function to execute arbitrary code through t SetAbortProc ... **Platforms**: win **CVEs**: CVE-2005-4560 **Refs**: source, ref1
MS06-013 Microsoft Internet Explorer createTextRange() Code Execution exploit/windows/browser/ms06_013_createtextrange	2006-03-19	normal	This module exploits a code execution vulnerability in Microsoft Internet Explorer. IE6 and IE7 (Beta 2) are vulnerable. It will corrupt memory in a way, which, under cer circumstances, can ... **Platforms**: win **CVEs**: CVE-2006-1359 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
MS06-055 Microsoft Internet Explorer VML Fill Method Code Execution exploit/windows/browser/ms06_055_vml_method	2006-09-19	normal	This module exploits a code execution vulnerability in Microsoft Internet Explorer u a buffer overflow in the VML processing co (VGX.dll). This module has been tested on Windows 2000 SP4, ... **Platforms**: win **CVEs**: CVE-2006-4868 **Refs**: source
MS06-067 Microsoft Internet Explorer Daxctle.OCX KeyFrame Method Heap Buffer Overflow Vulnerability exploit/windows/browser/ms06_067_keyframe	2006-11-14	normal	This module exploits a heap overflow vulnerability in the KeyFrame method of th direct animation ActiveX control. This is a p the exploit implemented by Alexander Soti **Platforms**: win **CVEs**: CVE-2006-4777 **Refs**: source
MS06-071 Microsoft Internet Explorer XML Core Services HTTP Request Handling exploit/windows/browser/ms06_071_xml_core	2006-10-10	normal	This module exploits a code execution vulnerability in Microsoft XML Core Service which exists in the XMLHTTP ActiveX cont This module is the modified version of ... **Platforms**: win **CVEs**: CVE-2006-5745 **Refs**: source
Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP) exploit/windows/browser/ms07_017_ani_loadimage_chunksize	2007-03-28	great	This module exploits a buffer overflow vulnerability in the LoadAniIcon() function i USER32.dll. The flaw can be triggered thro Internet Explorer 6 and 7 by using the CUR style sheet directive ... **Platforms**: win **CVEs**: CVE-2007-0038 **Refs**: source
Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download exploit/windows/browser/ms08_041_snapshotviewer	2008-07-07	excellent	This module allows remote attackers to pla arbitrary files on a users file system via the Microsoft Office Snapshot Viewer ActiveX Control. **Platforms**: win **CVEs**: CVE-2008-2463 **Refs**: source
Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow exploit/windows/browser/ms08_053_mediaencoder	2008-09-09	normal	This module exploits a stack buffer overflo Windows Media Encoder 9. When sending overly long string to the GetDetailsString() method of wmex.dll an attacker may be ab execute arbitrary ... **Platforms**: win **CVEs**: CVE-2008-3008 **Refs**: source
Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow exploit/windows/browser/ms08_070_visual_studio_msmask	2008-08-13	normal	This module exploits a stack buffer overflo Microsoft's Visual Studio 6.0. When passin specially crafted string to the Mask parame the Mdmask32.ocx ActiveX Control, an atta may be ... **Platforms**: win **CVEs**: CVE-2008-3704 **Refs**: source
MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption exploit/windows/browser/ms08_078_xml_corruption	2008-12-07	normal	This module exploits a vulnerability in the d binding feature of Internet Explorer. In orde execute code reliably, this module uses the .NET DLL memory technique pioneered by Alexander Sotirov ... **Platforms**: win **CVEs**: CVE-2008-4844 **Refs**: source, ref1
MS09-002 Microsoft Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption exploit/windows/browser/ms09_002_memory_corruption	2009-02-10	normal	This module exploits an error related to the CFunctionPointer function when attempting access uninitialized memory. A remote atta could exploit this vulnerability to corrupt me and execute ... **Platforms**: win **CVEs**: CVE-2009-0075 **Refs**: source

Metasploit Module	Date	Rank	Details
Microsoft OWC Spreadsheet HTMLURL Buffer Overflow exploit/windows/browser/ms09_043_owc_htmlurl	2009-08-11	normal	This module exploits a buffer overflow in Microsoft's Office Web Components. Wher passing an overly long string as the "HTML parameter an attacker can execute arbitrar code. **Platforms**: win **CVEs**: CVE-2009-1534 **Refs**: source, ref1
Microsoft OWC Spreadsheet msDataSourceObject Memory Corruption exploit/windows/browser/ms09_043_owc_msdso	2009-07-13	normal	This module exploits a memory corruption vulnerability within versions 10 and 11 of th Office Web Component Spreadsheet Activ control. This module was based on an exp found in the wild. **Platforms**: win **CVEs**: CVE-2009-1136 **Refs**: source, ref1, ref2
MS09-072 Microsoft Internet Explorer Style getElementsByTagName Memory Corruption exploit/windows/browser/ms09_072_style_object	2009-11-20	normal	This module exploits a vulnerability in the getElementsByTagName function as implemented within Internet Explorer. **Platforms**: win **CVEs**: CVE-2009-3672 **Refs**: source, ref1
MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption exploit/windows/browser/ms10_002_aurora	2010-01-14	normal	This module exploits a memory corruption in Internet Explorer. This flaw was found in wild and was a key component of the "Ope Aurora" attacks that lead to the compromis number ... **Platforms**: win **CVEs**: CVE-2010-0249 **Refs**: source, ref1
MS10-002 Microsoft Internet Explorer Object Memory Use-After-Free exploit/windows/browser/ms10_002_ie_object	2010-01-21	normal	This module exploits a vulnerability found i Internet Explorer's mshtml component. Du the way IE handles objects in memory, it is possible to cause a pointer in ... **Platforms**: win **CVEs**: CVE-2010-0248 **Refs**: source, ref1
MS10-018 Microsoft Internet Explorer DHTML Behaviors Use After Free exploit/windows/browser/ms10_018_ie_behaviors	2010-03-09	good	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 ... **Platforms**: win **CVEs**: CVE-2010-0806 **Refs**: source, ref1, ref2
MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution exploit/windows/browser/ms10_022_ie_vbscript_winhlp32	2010-02-26	great	This module exploits a code execution vulnerability that occurs when a user press on MessageBox originated from VBscript v a web page. When the user hits F1, the MessageBox help ... **Platforms**: win **CVEs**: CVE-2010-0483 **Refs**: source, ref1, ref2
MS10-026 Microsoft MPEG Layer-3 Audio Stack Based Overflow exploit/windows/browser/ms10_026_avi_nsamplespersec	2010-04-13	normal	This module exploits a buffer overflow in l3codecx.ax while processing a AVI files wi MPEG Layer-3 audio contents. The overflo only allows to overwrite with 0's so the thre least significant ... **Platforms**: win **CVEs**: CVE-2010-0480 **Refs**: source, ref1, ref2
Microsoft Help Center XSS and Command Execution exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec	2010-06-09	excellent	Help and Support Center is the default application provided to access online documentation for Microsoft Windows. Mic supports accessing help documents directl URLs by installing a ... **Platforms**: win **CVEs**: CVE-2010-1885 **Refs**: source

Metasploit Module	Date	Rank	Details
Microsoft Windows Shell LNK Code Execution exploit/windows/browser/ms10_046_shortcut_icon_dllloader	2010-07-16	excellent	This module exploits a vulnerability in the handling of Windows Shortcut files (.LNK) f contain an icon resource pointing to a mali DLL. This module creates a WebDAV servi that can be used ... **Platforms**: win **CVEs**: CVE-2010-2568 **Refs**: source
MS10-090 Microsoft Internet Explorer CSS SetUserClip Memory Corruption exploit/windows/browser/ms10_090_ie_css_clip	2010-11-03	good	This module exploits a memory corruption vulnerability within Microsoft's HTML engin (mshtml). When parsing an HTML page containing a specially crafted CSS tag, me corruption occurs that can ... **Platforms**: win **CVEs**: CVE-2010-3962 **Refs**: source
MS11-003 Microsoft Internet Explorer CSS Recursive Import Use After Free exploit/windows/browser/ms11_003_ie_css_import	2010-11-29	good	This module exploits a memory corruption vulnerability within Microsoft's HTML engin (mshtml). When parsing an HTML page containing a recursive CSS import, a C++ o is deleted and later reused. ... **Platforms**: win **CVEs**: CVE-2010-3971 **Refs**: source, ref1, ref2
MS11-050 IE mshtml!CObjectElement Use After Free exploit/windows/browser/ms11_050_mshtml_cobjectelement	2011-06-16	normal	This module exploits a use-after-free vulnerability in Internet Explorer. The vulnerability occurs when an invalid
MS11-081 Microsoft Internet Explorer Option Element Use-After-Free exploit/windows/browser/ms11_081_option	2012-10-11	normal	This module exploits a vulnerability in Micr Internet Explorer. A memory corruption ma occur when the Option cache isn't updated properly, which allows other JavaScript me to access a ... **Platforms**: win **CVEs**: CVE-2011-1996 **Refs**: source, ref1, ref2
MS11-093 Microsoft Windows OLE Object File Handling Remote Code Execution exploit/windows/browser/ms11_093_ole32	2011-12-13	normal	This module exploits a type confusion vulnerability in the OLE32 component of Windows XP SP3. The vulnerability exists CPropertyStorage::ReadMultiple function. A Visio document with a ... **Platforms**: win **CVEs**: CVE-2011-3400 **Refs**: source, ref1, ref2
MS12-004 midiOutPlayNextPolyEvent Heap Overflow exploit/windows/browser/ms12_004_midi	2012-01-10	normal	This module exploits a heap overflow vulnerability in the Windows Multimedia Lib (winmm.dll). The vulnerability occurs when parsing specially crafted MIDI files. Remot code execution can be ... **Platforms**: win **CVEs**: CVE-2012-0003 **Refs**: source
MS12-037 Microsoft Internet Explorer Fixed Table Col Span Heap Overflow exploit/windows/browser/ms12_037_ie_colspan	2012-06-12	normal	This module exploits a heap overflow vulnerability in Internet Explorer caused by incorrect handling of the span attribute for elements from a fixed table, when they are modified dynamically ... **Platforms**: win **CVEs**: CVE-2012-1876 **Refs**: source
MS12-037 Microsoft Internet Explorer Same ID Property Deleted Object Handling Memory Corruption exploit/windows/browser/ms12_037_same_id	2012-06-12	normal	This module exploits a memory corruption in Internet Explorer 8 when handling object with the same ID property. At the moment t module targets IE8 over Windows XP SP3 Windows 7. This ... **Platforms**: win **CVEs**: CVE-2012-1875 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
MS13-009 Microsoft Internet Explorer SLayoutRun Use-After-Free exploit/windows/browser/ms13_009_ie_slayoutrun_uaf	2013-02-13	average	This module exploits a use-after-free vulnerability in Microsoft Internet Explorer v a CParaElement node is released but a reference is still kept in CDoc. This memor reused when a CDoc ... **Platforms**: win **CVEs**: CVE-2013-0025 **Refs**: source, ref1
MS13-022 Microsoft Silverlight ScriptObject Unsafe Memory Access exploit/windows/browser/ms13_022_silverlight_script_object	2013-03-12	normal	This module exploits a vulnerability in Micr Silverlight. The vulnerability exists on the Initialize() method from System.Windows.Browser.ScriptObject, wh access memory in an unsafe manner. ... **Platforms**: win **CVEs**: CVE-2013-0074, CVE-2013-3896 **Refs**: source
MS13-055 Microsoft Internet Explorer CAnchorElement Use-After-Free exploit/windows/browser/ms13_055_canchor	2013-07-09	normal	In IE8 standards mode, it's possible to cau use-after-free condition by first creating an illogical table tree, where a CPhraseEleme comes after CTableRow, with the final node being a sub table ... **Platforms**: win **CVEs**: CVE-2013-3163 **Refs**: source, ref1
MS13-059 Microsoft Internet Explorer CFlatMarkupPointer Use-After-Free exploit/windows/browser/ms13_059_cflatmarkuppointer	2013-06-27	normal	This is a memory corruption bug found in Microsoft Internet Explorer. On IE 9, it seer only affect certain releases of mshtml.dll, ranging from a newly installed IE9 (9.0.8112.16446), to ... **Platforms**: win **CVEs**: CVE-2013-3184 **Refs**: source
MS13-069 Microsoft Internet Explorer CCaret Use-After-Free exploit/windows/browser/ms13_069_caret	2013-09-10	normal	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 ... **Platforms**: win **CVEs**: CVE-2013-3205 **Refs**: source
MS13-080 Microsoft Internet Explorer CDisplayPointer Use-After-Free exploit/windows/browser/ms13_080_cdisplaypointer	2013-10-08	normal	This module exploits a vulnerability found i Microsoft Internet Explorer. It was originally found being exploited in the wild targeting Japanese and Korean IE8 users on Windo XP, around the same ... **Platforms**: win **CVEs**: CVE-2013-3893, CVE-2013-3897 **Refs**: source, ref1, ref2
MS13-090 CardSpaceClaimCollection ActiveX Integer Underflow exploit/windows/browser/ms13_090_cardspacesigninhelper	2013-11-08	normal	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. ... **Platforms**: win **CVEs**: CVE-2013-3918 **Refs**: source, ref1
MS14-012 Microsoft Internet Explorer CMarkup Use-After-Free exploit/windows/browser/ms14_012_cmarkup_uaf	2014-02-13	normal	This module exploits an use after free conc on Internet Explorer as used in the wild as of "Operation SnowMan" in February 2014 module uses Flash Player 12 in order to by ASLR and ... **Platforms**: win **CVEs**: CVE-2014-0322 **Refs**: source, ref1, ref2
MS14-012 Microsoft Internet Explorer TextRange Use-After-Free exploit/windows/browser/ms14_012_textrange	2014-03-11	normal	This module exploits a use-after-free vulnerability found in Internet Explorer. The was most likely introduced in 2013, therefo only certain builds of MSHTML are affected our testing with ... **Platforms**: win **CVEs**: CVE-2014-0307 **Refs**: source

Metasploit Module	Date	Rank	Details
MS14-064 Microsoft Internet Explorer Windows OLE Automation Array Remote Code Execution exploit/windows/browser/ms14_064_ole_code_execution	2014-11-13	good	This module exploits the Windows OLE Automation array vulnerability, CVE-2014-6 The vulnerability is known to affect Internet Explorer 3.0 until version 11 within Window up to Windows 10, and ... **Platforms**: win **CVEs**: CVE-2014-6332 **Refs**: source, ref1, ref2
Internet Explorer 11 VBScript Engine Memory Corruption exploit/windows/browser/ms16_051_vbscript	2016-05-10	normal	This module exploits the memory corruptio vulnerability (CVE-2016-0189) present in th VBScript engine of Internet Explorer 11. **Platforms**: win **CVEs**: CVE-2016-0189 **Refs**: source
Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory Corruption exploit/windows/browser/msvidctl_mpeg2	2009-07-05	normal	This module exploits a memory corruption the MSVidCtl component of Microsoft DirectShow (BDATuner.MPEG2TuneReque By loading a specially crafted GIF file, an attacker can overrun a buffer ... **Platforms**: win **CVEs**: CVE-2008-0015 **Refs**: source
Microsoft Whale Intelligent Application Gateway ActiveX Control Buffer Overflow exploit/windows/browser/mswhale_checkforupdates	2009-04-15	normal	This module exploits a stack buffer overflo Microsoft Whale Intelligent Application Gat Whale Client. When sending an overly long string to CheckForUpdates() method of WhlMgr.dll (3.1.502.64) ... **Platforms**: win **CVEs**: CVE-2007-2238 **Refs**: source, ref1
MS12-043 Microsoft XML Core Services MSXML Uninitialized Memory Corruption exploit/windows/browser/msxml_get_definition_code_exec	2012-06-12	good	This module exploits a memory corruption in Microsoft XML Core Services when tryin access an uninitialized Node with the getDefinition API, which may corrupt memo allowing remote code ... **Platforms**: win **CVEs**: CVE-2012-1889 **Refs**: source, ref1, ref2, ref3
NCTAudioFile2 v2.x ActiveX Control SetFormatLikeSample() Buffer Overflow exploit/windows/browser/nctaudiofile2_setformatlikesample	2007-01-24	normal	This module exploits a stack buffer overflo the NCTAudioFile2.Audio ActiveX Control provided by various audio applications. By sending an overly long string to the "SetFormatLikeSample()" method, ... **Platforms**: win **CVEs**: CVE-2007-0018 **Refs**: source
Norton AntiSpam 2004 SymSpamHelper ActiveX Control Buffer Overflow exploit/windows/browser/nis2004_antispam	2004-03-19	normal	This module exploits a stack buffer overflo Norton AntiSpam 2004. When sending an long string to the LaunchCustomRuleWizar method of symspam.dll (2004.1.0.147) an attacker may be able ... **Platforms**: win **CVEs**: CVE-2004-0363 **Refs**: source
IBM Lotus Notes Client URL Handler Command Injection exploit/windows/browser/notes_handler_cmdinject	2012-06-18	excellent	This module exploits a command injection vulnerability in the URL handler for for the Lotus Notes Client <= 8.5.3. The registered handler can be abused with a specially cra notes:// URL to ... **Platforms**: win **CVEs**: CVE-2012-2174 **Refs**: source, ref1, ref2
Novell iPrint Client ActiveX Control call-back-url Buffer Overflow exploit/windows/browser/novelliprint_callbackurl	2010-08-20	normal	This module exploits a stack-based buffer overflow in Novell iPrint Client 5.42. When sending an overly long string to the 'call-ba url' parameter in an op-client-interface-vers action of ... **Platforms**: win **CVEs**: CVE-2010-1527 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Novell iPrint Client ActiveX Control Date/Time Buffer Overflow exploit/windows/browser/novelliprint_datetime	2009-12-08	great	This module exploits a stack buffer overflo Novell iPrint Client 5.30. When passing a specially crafted date/time string via certair parameters to ienipp.ocx an attacker can execute arbitrary ... **Platforms**: win **CVEs**: CVE-2009-1569 **Refs**: source, ref1
Novell iPrint Client ActiveX Control ExecuteRequest Buffer Overflow exploit/windows/browser/novelliprint_executerequest	2008-02-22	normal	This module exploits a stack buffer overflo Novell iPrint Client 4.26. When sending an overly long string to the ExecuteRequest() property of ienipp.ocx an attacker may be a to execute ... **Platforms**: win **CVEs**: CVE-2008-0935 **Refs**: source
Novell iPrint Client ActiveX Control ExecuteRequest debug Buffer Overflow exploit/windows/browser/novelliprint_executerequest_dbg	2010-08-04	normal	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 ... **Platforms**: win **CVEs**: CVE-2010-3106 **Refs**: source, ref1
Novell iPrint Client ActiveX Control Buffer Overflow exploit/windows/browser/novelliprint_getdriversettings	2008-06-16	normal	This module exploits a stack buffer overflo Novell iPrint Client 4.34. When sending an overly long string to the GetDriverSettings(property of ienipp.ocx an attacker may be a to execute ... **Platforms**: win **CVEs**: CVE-2008-2908 **Refs**: source, ref1
Novell iPrint Client ActiveX Control Buffer Overflow exploit/windows/browser/novelliprint_getdriversettings_2	2010-11-15	normal	This module exploits a stack buffer overflo Novell iPrint Client 5.52. When sending an overly long string to the GetDriverSettings(property of ienipp.ocx an attacker may be a to execute ... **Platforms**: win **CVEs**: CVE-2010-4321 **Refs**: source, ref1
Novell iPrint Client ActiveX Control target-frame Buffer Overflow exploit/windows/browser/novelliprint_target_frame	2009-12-08	great	This module exploits a stack buffer overflo Novell iPrint Client 5.30. When passing an overly long string via the "target-frame" parameter to ienipp.ocx an attacker can ex arbitrary code. ... **Platforms**: win **CVEs**: CVE-2009-1568 **Refs**: source, ref1
Novell GroupWise Client gwcls1.dll ActiveX Remote Code Execution exploit/windows/browser/novell_groupwise_gwcls1_actvx	2013-01-30	normal	This module exploits a vulnerability in the N GroupWise Client gwcls1.dll ActiveX. Seve methods in the GWCalServer control use u provided data as a pointer, which allows to arbitrary ... **Platforms**: win **CVEs**: CVE-2012-0439 **Refs**: source, ref1
NTR ActiveX Control Check() Method Buffer Overflow exploit/windows/browser/ntr_activex_check_bof	2012-01-11	normal	This module exploits a vulnerability found i NTR ActiveX 1.1.8. The vulnerability exists the Check() method, due to the insecure us of strcat to build a URL using the bstrParar parameter ... **Platforms**: win **CVEs**: CVE-2012-0266 **Refs**: source, ref1
NTR ActiveX Control StopModule() Remote Code Execution exploit/windows/browser/ntr_activex_stopmodule	2012-01-11	normal	This module exploits a vulnerability found i NTR ActiveX 1.1.8. The vulnerability exists the StopModule() method, where the lModu parameter is used to dereference memory a function ... **Platforms**: win **CVEs**: CVE-2012-0267 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Oracle AutoVue ActiveX Control SetMarkupMode Buffer Overflow exploit/windows/browser/oracle_autovue_setmarkupmode	2012-04-18	normal	This module exploits a vulnerability found i AutoVue.ocx ActiveX control. The vulnerab due to the insecure usage of an strcpy like function in the SetMarkupMode method, w handling a ... **Platforms**: win **CVEs**: CVE-2012-0549 **Refs**: source, ref1, ref2, ref3
Oracle Document Capture 10g ActiveX Control Buffer Overflow exploit/windows/browser/oracle_dc_submittoexpress	2009-08-28	normal	This module exploits a stack buffer overflo Oracle Document Capture 10g (10.1.3.5.0) Oracle Document Capture 10g comes bun with a third party ActiveX control emsmtp.d (6.0.1.0). When ... **Platforms**: win **CVEs**: CVE-2007-4607 **Refs**: source
Oracle WebCenter Content CheckOutAndOpen.dll ActiveX Remote Code Execution exploit/windows/browser/oracle_webcenter_checkoutandopen	2013-04-16	excellent	This module exploits a vulnerability found i Oracle WebCenter Content CheckOutAndOpenControl ActiveX. This vulnerability exists in openWebdav(), wher user controlled input is used to call ... **Platforms**: win **CVEs**: CVE-2013-1559 **Refs**: source, ref1
VMWare OVF Tools Format String Vulnerability exploit/windows/browser/ovftool_format_string	2012-11-08	normal	This module exploits a format string vulner in VMWare OVF Tools 2.1 for Windows. Th vulnerability occurs when printing error messages while parsing a a malformed OV file. The module has been ... **Platforms**: win **CVEs**: CVE-2012-3569 **Refs**: source, ref1
PcVue 10.0 SV.UIGrdCtrl.1 'LoadObject()/SaveObject()' Trusted DWORD Vulnerability exploit/windows/browser/pcvue_func	2011-10-05	average	This module exploits a function pointer con within SVUIGrd.ocx of PcVue 10.0. By sett dword value for the SaveObject() or LoadObject(), an attacker can overwrite a function pointer and ... **Platforms**: win **CVEs**: CVE-2011-4044 **Refs**: source, ref1
Persits XUpload ActiveX MakeHttpRequest Directory Traversal exploit/windows/browser/persits_xupload_traversal	2009-09-29	excellent	This module exploits a directory traversal i Persits Software Inc's XUpload ActiveX control(version 3.0.0.3) that's included in H LoadRunner 9.5. By passing a string conta ".\" sequences to ... **Platforms**: win **CVEs**: CVE-2009-3693 **Refs**: source
IBM Lotus QuickR qp2 ActiveX Buffer Overflow exploit/windows/browser/quickr_qp2_bof	2012-05-23	normal	This module exploits a buffer overflow vulnerability on the UploadControl ActiveX. vulnerability exists in the handling of the "Attachment_Times" property, due to the insecure usage of the ... **Platforms**: win **CVEs**: CVE-2012-2176 **Refs**: source, ref1
RealNetworks RealPlayer CDDA URI Initialization Vulnerability exploit/windows/browser/realplayer_cdda_uri	2010-11-15	normal	This module exploits an initialization flaw w RealPlayer 11/11.1 and RealPlayer SP 1.0 1.1.4. An abnormally long CDDA URI caus object initialization failure. However, this fa is ... **Platforms**: win **CVEs**: CVE-2010-3747 **Refs**: source, ref1
RealPlayer rmoc3260.dll ActiveX Control Heap Corruption exploit/windows/browser/realplayer_console	2008-03-08	normal	This module exploits a heap corruption vulnerability in the RealPlayer ActiveX cont By sending a specially crafted string to the 'Console' property in the rmoc3260.dll cont an attacker may be ... **Platforms**: win **CVEs**: CVE-2008-1309 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
RealPlayer ierpplug.dll ActiveX Control Playlist Name Buffer Overflow exploit/windows/browser/realplayer_import	2007-10-18	normal	This module exploits a stack buffer overflo RealOne Player V2 Gold Build 6.0.11.853 a RealPlayer 10.5 Build 6.0.12.1483. By sen an overly long string to the "Import()" meth an attacker ... **Platforms**: win **CVEs**: CVE-2007-5601 **Refs**: source
RealNetworks Realplayer QCP Parsing Heap Overflow exploit/windows/browser/realplayer_qcp	2011-08-16	average	This module exploits a heap overflow in Realplayer when handling a .QCP file. The specific flaw exists within qcpfformat.dll. A 256 byte buffer is allocated on the heap an user-supplied data ... **Platforms**: win **CVEs**: CVE-2011-2950 **Refs**: source, ref1
RealNetworks RealPlayer SMIL Buffer Overflow exploit/windows/browser/realplayer_smil	2005-03-01	normal	This module exploits a stack buffer overflo RealNetworks RealPlayer 10 and 8. By cre a URL link to a malicious SMIL file, a remo attacker could overflow a buffer and execu arbitrary ... **Platforms**: win **CVEs**: CVE-2005-0455 **Refs**: source
Real Networks Arcade Games StubbyUtil.ProcessMgr ActiveX Arbitrary Code Execution exploit/windows/browser/real_arcade_installerdlg	2011-04-03	normal	This module exploits a vulnerability in Real Networks Arcade Game's ActiveX control. "exec" function found in InstallerDlg.dll (v2.6.0.445) allows remote attackers to run arbitrary commands on ... **Platforms**: win **Refs**: source
Roxio CinePlayer ActiveX Control Buffer Overflow exploit/windows/browser/roxio_cineplayer	2007-04-11	normal	This module exploits a stack-based buffer overflow in SonicPlayer ActiveX control (SonicMediaPlayer.dll) 3.0.0.1 installed by CinePlayer 3.2. By setting an overly long v to 'DiskType', an ... **Platforms**: win **CVEs**: CVE-2007-1559 **Refs**: source
Apple Safari Webkit libxslt Arbitrary File Creation exploit/windows/browser/safari_xslt_output	2011-07-20	excellent	This module exploits a file creation vulnera in the Webkit rendering engine. It is possib redirect the output of a XSLT transformatio an arbitrary file. The content of the created ... **Platforms**: win **CVEs**: CVE-2011-1774 **Refs**: source, ref1
Samsung NET-i Viewer Multiple ActiveX BackupToAvi() Remote Overflow exploit/windows/browser/samsung_neti_wiewer_backuptoavi_bof	2012-04-21	normal	This module exploits a vulnerability in the CNC_Ctrl.dll ActiveX control installed with Samsung NET-i viewer 1.37. Specifically, v supplying a long string for the fname paran to the ... **Platforms**: win **CVEs**: CVE-2012-4333 **Refs**: source, ref1
Samsung Security Manager 1.4 ActiveMQ Broker Service PUT Method Remote Code Execution exploit/windows/browser/samsung_security_manager_put	2016-08-05	excellent	This is an exploit against Samsung Securit Manager that bypasses the patch in ZDI-15 ZDI-16-481 by exploiting the vulnerability against the client-side. This exploit has bee tested ... **Platforms**: win **Refs**: source, ref1, ref2
Siemens Solid Edge ST4 SEListCtrlX ActiveX Remote Code Execution exploit/windows/browser/siemens_solid_edge_selistctrlx	2013-05-26	normal	This module exploits the SEListCtrlX Active installed with the Siemens Solid Edge prod The vulnerability exists on several APIs provided by the control, where user supplie input is handled as a ... **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
SoftArtisans XFile FileManager ActiveX Control Buffer Overflow exploit/windows/browser/softartisans_getdrivename	2008-08-25	normal	This module exploits a stack buffer overflo SoftArtisans XFile FileManager ActiveX co (SAFmgPwd.dll 2.0.5.3). When sending an overly long string to the GetDriveName() method an attacker may ... **Platforms**: win **CVEs**: CVE-2007-1682 **Refs**: source
SonicWall SSL-VPN NetExtender ActiveX Control Buffer Overflow exploit/windows/browser/sonicwall_addrouteentry	2007-11-01	normal	This module exploits a stack buffer overflo SonicWall SSL-VPN NetExtender. By send an overly long string to the "AddRouteEntry method located in the NELaunchX.dll (1.0. Control, an ... **Platforms**: win **CVEs**: CVE-2007-5603 **Refs**: source, ref1
Symantec Altiris Deployment Solution ActiveX Control Arbitrary File Download and Execute exploit/windows/browser/symantec_altirisdeployment_downloadandinstall	2009-09-09	excellent	This module allows remote attackers to ins and execute arbitrary files on a users file s via AeXNSPkgDLLib.dll (6.0.0.1418). This module was tested against Symantec Altiri Deployment ... **Platforms**: win **CVEs**: CVE-2009-3028 **Refs**: source
Symantec Altiris Deployment Solution ActiveX Control Buffer Overflow exploit/windows/browser/symantec_altirisdeployment_runcmd	2009-11-04	normal	This module exploits a stack buffer overflo Symantec Altiris Deployment Solution. Wh sending an overly long string to RunCmd() method of AeXNSConsoleUtilities.dll (6.0.0.1426) an attacker may ... **Platforms**: win **CVEs**: CVE-2009-3033 **Refs**: source
Symantec AppStream LaunchObj ActiveX Control Arbitrary File Download and Execute exploit/windows/browser/symantec_appstream_unsafe	2009-01-15	excellent	This module exploits a vulnerability in Sym AppStream Client 5.x. The vulnerability is i LaunchObj ActiveX control (launcher.dll 5.1.0.82) containing the "installAppMgr()" method. The ... **Platforms**: win **CVEs**: CVE-2008-4388 **Refs**: source
Symantec BackupExec Calendar Control Buffer Overflow exploit/windows/browser/symantec_backupexec_pvcalendar	2008-02-28	normal	This module exploits a stack buffer overflo Symantec BackupExec Calendar Control. I sending an overly long string to the "_DOWText0" property located in the pvcalendar.ocx control, an attacker ... **Platforms**: win **CVEs**: CVE-2007-6016 **Refs**: source, ref1
Symantec ConsoleUtilities ActiveX Control Buffer Overflow exploit/windows/browser/symantec_consoleutilities_browseandsavefile	2009-11-02	normal	This module exploits a stack buffer overflo Symantecs ConsoleUtilities. By sending ar overly long string to the "BrowseAndSaveF method located in the AeXNSConsoleUtilit (6.0.0.1846) ... **Platforms**: win **CVEs**: CVE-2009-3031 **Refs**: source, ref1, ref2
Synactis PDF In-The-Box ConnectToSynactic Stack Buffer Overflow exploit/windows/browser/synactis_connecttosynactis_bof	2013-05-30	normal	This module exploits a vulnerability found i Synactis' PDF In-The-Box ActiveX compon specifically PDF_IN_1.ocx. When a long st of data is given to the ConnectToSynactis function, which is ... **Platforms**: win **Refs**: source
Husdawg, LLC. System Requirements Lab ActiveX Unsafe Method exploit/windows/browser/systemrequirementslab_unsafe	2008-10-16	excellent	This module allows attackers to execute co via an unsafe method in Husdawg, LLC. Sy Requirements Lab ActiveX Control (sysreqlab2.dll 2.30.0.0). **Platforms**: win **CVEs**: CVE-2008-4385 **Refs**: source

Metasploit Module	Date	Rank	Details
TeeChart Professional ActiveX Control Trusted Integer Dereference exploit/windows/browser/teechart_pro	2011-08-11	normal	This module exploits an integer overflow in TeeChart Pro ActiveX control. When sendi overly large/negative integer value to the AddSeries() property of TeeChart2010.ocx code will perform an ... **Platforms**: win **Refs**: source, ref1
Tom Sawyer Software GET Extension Factory Remote Code Execution exploit/windows/browser/tom_sawyer_tsgetx71ex552	2011-05-03	normal	This module exploits a remote code execut vulnerability in the tsgetx71ex553.dll Active control installed with Tom Sawyer GET Extension Factory due to an incorrect initialization under Internet ... **Platforms**: win **CVEs**: CVE-2011-2217 **Refs**: source, ref1
Trend Micro Internet Security Pro 2010 ActiveX extSetOwner() Remote Code Execution exploit/windows/browser/trendmicro_extsetowner	2010-08-25	normal	This module exploits a remote code execut vulnerability in Trend Micro Internet Securit 2010 ActiveX. When sending an invalid po to the extSetOwner() function of UfPBCtrl.c attacker ... **Platforms**: win **CVEs**: CVE-2010-3189 **Refs**: source
Trend Micro OfficeScan Client ActiveX Control Buffer Overflow exploit/windows/browser/trendmicro_officescan	2007-02-12	normal	This module exploits a stack buffer overflo Trend Micro OfficeScan Corporate Edition By sending an overly long string to the "CgiOnUpdate()" method located in the OfficeScanSetupINI.dll ... **Platforms**: win **CVEs**: CVE-2007-0325 **Refs**: source
Ubisoft uplay 2.0.3 ActiveX Control Arbitrary Code Execution exploit/windows/browser/ubisoft_uplay_cmd_exec	2012-07-29	normal	The uplay ActiveX component allows an attacker to execute any command line acti User must sign in, unless auto-sign in is enabled and uplay must not already be run Due to the way the ... **Platforms**: win **CVEs**: CVE-2012-4177 **Refs**: source, ref1, ref2
TRENDnet SecurView Internet Camera UltraMJCam OpenFileDlg Buffer Overflow exploit/windows/browser/ultramjcam_openfiledig_bof	2012-03-28	normal	This module exploits a vulnerability found i TRENDnet SecurView Internet Camera's ActiveX control. By supplying a long string data as the sFilter argument of the OpenFileDlg() function, it is ... **Platforms**: win **CVEs**: CVE-2012-4876 **Refs**: source
Ultra Shareware Office Control ActiveX HttpUpload Buffer Overflow exploit/windows/browser/ultraoffice_httpupload	2008-08-27	good	This module exploits a stack-based buffer overflow in Ultra Shareware's Office Contro When processing the 'HttpUpload' method, arguments are concatenated together to fo command line to run ... **Platforms**: win **CVEs**: CVE-2008-3878 **Refs**: source
VeryPDF PDFView OCX ActiveX OpenPDF Heap Overflow exploit/windows/browser/verypdf_pdfview	2008-06-16	normal	The VeryPDF PDFView ActiveX control is p 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 ... **Platforms**: win **CVEs**: CVE-2008-5492 **Refs**: source
Viscom Software Movie Player Pro SDK ActiveX 6.8 exploit/windows/browser/viscom_movieplayer_drawtext	2010-01-12	normal	Stack-based buffer overflow in the MOVIEPLAYER.MoviePlayerCtrl.1 ActiveX control in MoviePlayer.ocx 6.8.0.0 in Visco Software Movie Player Pro SDK ActiveX 6. allows remote attackers to execute ... **Platforms**: win **CVEs**: CVE-2010-0356 **Refs**: source

Metasploit Module	Date	Rank	Details
VLC AMV Dangling Pointer Vulnerability exploit/windows/browser/vlc_amv	2011-03-23	good	This module exploits VLC media player wh handling a .AMV file. By flipping the 0x41st in the file format (video width/height), VLC crashes due to an invalid pointer, which all remote ... **Platforms**: win **CVEs**: CVE-2010-3275 **Refs**: source, ref1, ref2
VLC MMS Stream Handling Buffer Overflow exploit/windows/browser/vlc_mms_bof	2012-03-15	normal	This module exploits a buffer overflow in V media player VLC media player prior to 2.0 The vulnerability is due to a dangerous use sprintf which can result in a stack buffer overflow when ... **Platforms**: win **CVEs**: CVE-2012-1775 **Refs**: source, ref1, ref2
WebDAV Application DLL Hijacker exploit/windows/browser/webdav_dll_hijacker	2010-08-18	manual	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 t specify a vulnerable application ... **Platforms**: win **Refs**: source, ref1, ref2
WebEx UCF atucfobj.dll ActiveX NewObject Method Buffer Overflow exploit/windows/browser/webex_ucf_newobject	2008-08-06	good	This module exploits a stack-based buffer overflow in WebEx's WebexUCFObject Act Control. If a long string is passed to the 'NewObject' method, a stack- based buffer overflow will occur when ... **Platforms**: win **CVEs**: CVE-2008-3558 **Refs**: source, ref1, ref2, ref3, ref4, ref5
KingScada kxClientDownload.ocx ActiveX Remote Code Execution exploit/windows/browser/wellintech_kingscada_kxclientdownload	2014-01-14	good	This module abuses the kxClientDownload ActiveX control distributed with WellingTec KingScada. The ProjectURL property can b abused to download and load arbitrary DLL from arbitrary locations, ... **Platforms**: win **CVEs**: CVE-2013-2827 **Refs**: source, ref1
Winamp Playlist UNC Path Computer Name Overflow exploit/windows/browser/winamp_playlist_unc	2006-01-29	great	This module exploits a vulnerability in the Winamp media player. This flaw is triggere when an audio file path is specified, inside playlist, that consists of a UNC path with a computer name. ... **Platforms**: win **CVEs**: CVE-2006-0476 **Refs**: source
Winamp Ultravox Streaming Metadata (in_mp3.dll) Buffer Overflow exploit/windows/browser/winamp_ultravox	2008-01-18	normal	This module exploits a stack buffer overflo Winamp 5.24. By sending an overly long a tag, a remote attacker may be able to exec arbitrary code. This vulnerability can be exploited from ... **Platforms**: win **CVEs**: CVE-2008-0065 **Refs**: source
WinDVD7 IASystemInfo.DLL ActiveX Control Buffer Overflow exploit/windows/browser/windvd7_applicationtype	2007-03-20	normal	This module exploits a stack buffer overflo IASystemInfo.dll ActiveX control in InterVid WinDVD 7. By sending an overly long strin the "ApplicationType()" property, an attacke may be able ... **Platforms**: win **CVEs**: CVE-2007-0348 **Refs**: source
WinZip FileView (WZFILEVIEW.FileViewCtrl.61) ActiveX Buffer Overflow exploit/windows/browser/winzip_fileview	2007-11-02	normal	The FileView ActiveX control (WZFILEVIEW.FileViewCtrl.61) could allow remote attacker to execute arbitrary code o system. The control contains several unsaf methods and is marked safe for ... **Platforms**: win **CVEs**: CVE-2006-5198 **Refs**: source

Metasploit Module	Date	Rank	Details
Microsoft WMI Administration Tools ActiveX Buffer Overflow exploit/windows/browser/wmi_admintools	2010-12-21	great	This module exploits a memory trust issue Microsoft WMI Administration tools ActiveX control. When processing a specially crafte HTML page, the WEBSingleView.ocx Activ Control (1.50.1131.0) ... **Platforms**: win **CVEs**: CVE-2010-3973 **Refs**: source, ref1, ref2, ref3
X360 VideoPlayer ActiveX Control Buffer Overflow exploit/windows/browser/x360_video_player_set_text_bof	2015-01-30	normal	This module exploits a buffer overflow in th VideoPlayer.ocx ActiveX installed with the Software. By setting an overly long value t 'ConvertFile()', an attacker can overrun a .c buffer to ... **Platforms**: win **Refs**: source, ref1
XMPlay 3.3.0.4 (ASX Filename) Buffer Overflow exploit/windows/browser/xmplay_asx	2006-11-21	good	This module exploits a stack buffer overflo XMPlay 3.3.0.4. The vulnerability is caused to a boundary error within the parsing of playlists containing an overly long file nam This module ... **Platforms**: win **CVEs**: CVE-2006-6063 **Refs**: source, ref1
Yahoo! Messenger YVerInfo.dll ActiveX Control Buffer Overflow exploit/windows/browser/yahoomessenger_fvcom	2007-08-30	normal	This module exploits a stack buffer overflo the Yahoo! Messenger ActiveX Control (YVerInfo.dll <= 2006.8.24.1). By sending a overly long string to the "fvCom()" method a yahoo.com domain, ... **Platforms**: win **CVEs**: CVE-2007-4515 **Refs**: source, ref1
Yahoo! Messenger 8.1.0.249 ActiveX Control Buffer Overflow exploit/windows/browser/yahoomessenger_server	2007-06-05	good	This module exploits a stack buffer overflo the Yahoo! Webcam Upload ActiveX Contr (ywcupl.dll) provided by Yahoo! Messenge version 8.1.0.249. By sending an overly lo string to the ... **Platforms**: win **CVEs**: CVE-2007-3147 **Refs**: source
Zenturi ProgramChecker ActiveX Control Arbitrary File Download exploit/windows/browser/zenturiprogramchecker_unsafe	2007-05-29	excellent	This module allows remote attackers to pla arbitrary files on a users file system via the Zenturi ProgramChecker sasatl.dll (1.5.0.5 ActiveX Control. **Platforms**: win **CVEs**: CVE-2007-2987 **Refs**: source
AdminStudio LaunchHelp.dll ActiveX Arbitrary Code Execution exploit/windows/browser/zenworks_helplauncher_exec	2011-10-19	normal	This module exploits a vulnerability in AdminStudio LaunchHelp.dll ActiveX contr The LaunchProcess function found in LaunchHelp.HelpLauncher.1 allows remote attackers to run arbitrary commands on ... **Platforms**: win **CVEs**: CVE-2011-2657 **Refs**: source, ref1
MS03-026 Microsoft RPC DCOM Interface Overflow exploit/windows/dcerpc/ms03_026_dcom	2003-07-16	great	This module exploits a stack buffer overflo the RPCSS service, this vulnerability was originally found by the Last Stage of Deliriu research group and has been widely explo ever since. This ... **Platforms**: win **CVEs**: CVE-2003-0352 **Refs**: source
MS05-017 Microsoft Message Queueing Service Path Overflow exploit/windows/dcerpc/ms05_017_msmq	2005-04-12	good	This module exploits a stack buffer overflo the RPC interface to the Microsoft Messag Queueing service. The offset to the return address changes based on the length of th system hostname, so ... **Platforms**: win **CVEs**: CVE-2005-0059 **Refs**: source

Metasploit Module	Date	Rank	Details
MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP) exploit/windows/dcerpc/ms07_029_msdns_zonename	2007-04-12	great	This module exploits a stack buffer overflo the RPC interface of the Microsoft DNS se The vulnerability is triggered when a long z name parameter is supplied that contains escaped octal ... **Platforms**: win **CVEs**: CVE-2007-1748 **Refs**: source
MS07-065 Microsoft Message Queueing Service DNS Name Path Overflow exploit/windows/dcerpc/ms07_065_msmq	2007-12-11	good	This module exploits a stack buffer overflo the RPC interface to the Microsoft Messag Queueing service. This exploit requires the target system to have been configured with DNS name and for ... **Platforms**: win **CVEs**: CVE-2007-3039 **Refs**: source
Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP) exploit/windows/email/ms07_017_ani_loadimage_chunksize	2007-03-28	great	This module exploits a buffer overflow vulnerability in the LoadAniIcon() function o USER32.dll. The flaw is triggered through Outlook Express by using the CURSOR sty sheet directive to load a ... **Platforms**: win **CVEs**: CVE-2007-0038, CVE-2007-1765 **Refs**: source
Outlook ATTACH_BY_REF_ONLY File Execution exploit/windows/email/ms10_045_outlook_ref_only	2010-06-01	excellent	It has been discovered that certain e-mail message cause Outlook to create Windows shortcut-like attachments or messages with Outlook. Through specially crafted TNEF streams with certain MAPI ... **Platforms**: win **CVEs**: CVE-2010-0266 **Refs**: source, ref1
Outlook ATTACH_BY_REF_RESOLVE File Execution exploit/windows/email/ms10_045_outlook_ref_resolve	2010-06-01	excellent	It has been discovered that certain e-mail message cause Outlook to create Windows shortcut-like attachments or messages with Outlook. Through specially crafted TNEF streams with certain MAPI ... **Platforms**: win **CVEs**: CVE-2010-0266 **Refs**: source, ref1
EMC AlphaStor Agent Buffer Overflow exploit/windows/emc/alphastor_agent	2008-05-27	great	This module exploits a stack buffer overflo EMC AlphaStor 3.1. By sending a specially crafted message, an attacker may be able execute arbitrary code. **Platforms**: win **CVEs**: CVE-2008-2158 **Refs**: source, ref1
EMC AlphaStor Device Manager Opcode 0x75 Command Injection exploit/windows/emc/alphastor_device_manager_exec	2013-01-18	excellent	This module exploits a flaw within the Devi Manager (rrobtd.exe). When parsing the 0x command, the process does not properly fi user supplied input allowing for arbitrary command injection. ... **Platforms**: win **CVEs**: CVE-2013-0928 **Refs**: source
EMC Networker Format String exploit/windows/emc/networker_format_string	2012-08-29	normal	This module exploits a format string vulner in the lg_sprintf function as implemented in liblocal.dll on EMC Networker products. Th module exploits the vulnerability by using a specially ... **Platforms**: win **CVEs**: CVE-2012-2288 **Refs**: source, ref1
EMC Replication Manager Command Execution exploit/windows/emc/replication_manager_exec	2011-02-07	great	This module exploits a remote command-injection vulnerability in EMC Replication Manager client (irccd.exe). By sending a specially crafted message invoking RunPro function an attacker may be ... **Platforms**: win **CVEs**: CVE-2011-0647 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
ABBS Audio Media Player .LST Buffer Overflow exploit/windows/fileformat/abbs_amp_lst	2013-06-30	normal	This module exploits a buffer overflow in A Audio Media Player. The vulnerability occu when adding a specially crafted .lst file, allo arbitrary code execution with the privileges the ... **Platforms**: win **Refs**: source
ACDSee FotoSlate PLP File id Parameter Overflow exploit/windows/fileformat/acdsee_fotoslate_string	2011-09-12	good	This module exploits a buffer overflow in ACDSee FotoSlate 4.0 Build 146 via a spe crafted id parameter in a String element. W viewing a malicious PLP file with the ACDS FotoSlate product, ... **Platforms**: win **CVEs**: CVE-2011-2595 **Refs**: source
ACDSee XPM File Section Buffer Overflow exploit/windows/fileformat/acdsee_xpm	2007-11-23	good	This module exploits a buffer overflow in ACDSee 9.0. When viewing a malicious XP file with the ACDSee product, a remote atta could overflow a buffer and execute arbitra code. **Platforms**: win **CVEs**: CVE-2007-2193 **Refs**: source
ActiveFax (ActFax) 4.3 Client Importer Buffer Overflow exploit/windows/fileformat/actfax_import_users_bof	2012-08-28	normal	This module exploits a vulnerability in Activ Server. The vulnerability is a stack based b overflow in the "Import Users from File" fun due to the insecure usage of strcpy while .. **Platforms**: win **Refs**: source, ref1
activePDF WebGrabber ActiveX Control Buffer Overflow exploit/windows/fileformat/activepdf_webgrabber	2008-08-26	low	This module exploits a stack buffer overflo activePDF WebGrabber 3.8. When sending overly long string to the GetStatus() metho APWebGrb.ocx (3.8.2.0) an attacker may b able to execute ... **Platforms**: win **Refs**: source, ref1
Adobe Collab.collectEmailInfo() Buffer Overflow exploit/windows/fileformat/adobe_collectemailinfo	2008-02-08	good	This module exploits a buffer overflow in A Reader and Adobe Acrobat Professional 8 By creating a specially crafted pdf that a contains malformed Collab.collectEmailInfo call, an attacker ... **Platforms**: win **CVEs**: CVE-2007-5659 **Refs**: source
Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow exploit/windows/fileformat/adobe_cooltype_sing	2010-09-07	great	This module exploits a vulnerability in the S INdependent Glyplets (SING) table handlin within versions 8.2.4 and 9.3.4 of Adobe Reader. Prior versions are assumed to be vulnerable as well. **Platforms**: win **CVEs**: CVE-2010-2883 **Refs**: source, ref1, ref2
Adobe Flash Player "Button" Remote Code Execution exploit/windows/fileformat/adobe_flashplayer_button	2010-10-28	normal	This module exploits a vulnerability in the handling of certain SWF movies within vers 9.x and 10.0 of Adobe Flash Player. Adobe Reader and Acrobat are also vulnerable, a any other ... **Platforms**: win **CVEs**: CVE-2010-3654 **Refs**: source, ref1, ref2, ref3
Adobe Flash Player "newfunction" Invalid Pointer Use exploit/windows/fileformat/adobe_flashplayer_newfunction	2010-06-04	normal	This module exploits a vulnerability in the DoABC tag handling within versions 9.x an 10.0 of Adobe Flash Player. Adobe Reader Acrobat are also vulnerable, as are any oth applications that may ... **Platforms**: win **CVEs**: CVE-2010-1297 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Adobe FlateDecode Stream Predictor 02 Integer Overflow exploit/windows/fileformat/adobe_flatedecode_predictor02	2009-10-08	good	This module exploits an integer overflow vulnerability in Adobe Reader and Adobe Acrobat Professional versions before 9.2. **Platforms**: win **CVEs**: CVE-2009-3459 **Refs**: source, ref1, ref2
Adobe Collab.getIcon() Buffer Overflow exploit/windows/fileformat/adobe_geticon	2009-03-24	good	This module exploits a buffer overflow in A Reader and Adobe Acrobat. Affected versi include < 7.1.1, < 8.1.3, and < 9.1. By crea specially crafted pdf that a contains malfor ... **Platforms**: win **CVEs**: CVE-2009-0927 **Refs**: source
Adobe Illustrator CS4 v14.0.0 exploit/windows/fileformat/adobe_illustrator_v14_eps	2009-12-03	great	Adobe Illustrator CS4 (V14.0.0) Encapsula Postscript (.eps) overlong DSC Comment E Overflow Exploit. **Platforms**: win **CVEs**: CVE-2009-4195 **Refs**: source
Adobe JBIG2Decode Memory Corruption exploit/windows/fileformat/adobe_jbig2decode	2009-02-19	good	This module exploits a heap-based pointer corruption flaw in Adobe Reader 9.0.0 and earlier. This module relies upon javascript f the heap spray. **Platforms**: win **CVEs**: CVE-2009-0658 **Refs**: source
Adobe Acrobat Bundled LibTIFF Integer Overflow exploit/windows/fileformat/adobe_libtiff	2010-02-16	good	This module exploits an integer overflow vulnerability in Adobe Reader and Adobe Acrobat Professional versions 8.0 through and 9.0 through 9.3. **Platforms**: win **CVEs**: CVE-2010-0188 **Refs**: source, ref1, ref2, ref3
Adobe Doc.media.newPlayer Use After Free Vulnerability exploit/windows/fileformat/adobe_media_newplayer	2009-12-14	good	This module exploits a use after free vulnerability in Adobe Reader and Adobe Acrobat Professional versions up to and including 9.2. **Platforms**: win **CVEs**: CVE-2009-4324 **Refs**: source
Adobe PDF Escape EXE Social Engineering (No JavaScript) exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs	2010-03-29	excellent	This module embeds a Metasploit payload an existing PDF file in a non-standard meth The resulting PDF can be sent to a target a part of a social engineering attack. **Platforms**: win **CVEs**: CVE-2010-1240 **Refs**: source, ref1, ref2, ref3, ref4
Adobe Reader U3D Memory Corruption Vulnerability exploit/windows/fileformat/adobe_reader_u3d	2011-12-06	average	This module exploits a vulnerability in the U handling within versions 9.x through 9.4.6 a 10 through to 10.1.1 of Adobe Reader. The vulnerability is due to the use of uninitialize memory. ... **Platforms**: win **CVEs**: CVE-2011-2462 **Refs**: source, ref1, ref2, ref3, ref4
Adobe Reader ToolButton Use After Free exploit/windows/fileformat/adobe_toolbutton	2013-08-08	normal	This module exploits a use after free condi on Adobe Reader versions 11.0.2, 10.1.6 a 9.5.4 and prior. The vulnerability exists whi handling the ToolButton object, where the cEnable callback ... **Platforms**: win **CVEs**: CVE-2013-3346 **Refs**: source, ref1, ref2
Adobe U3D CLODProgressiveMeshDeclaration Array Overrun exploit/windows/fileformat/adobe_u3d_meshdecl	2009-10-13	good	This module exploits an array overflow in A Reader and Adobe Acrobat. Affected versi include < 7.1.4, < 8.2, and < 9.3. By creatir specially crafted pdf that a contains malfor U3D data, ... **Platforms**: win **CVEs**: CVE-2009-3953 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Adobe util.printf() Buffer Overflow exploit/windows/fileformat/adobe_utilprintf	2008-02-08	good	This module exploits a buffer overflow in A Reader and Adobe Acrobat Professional < 8.1.3. By creating a specially crafted pdf th contains malformed util.printf() entry, an att may be ... **Platforms**: win **CVEs**: CVE-2008-2992 **Refs**: source
ALLPlayer M3U Buffer Overflow exploit/windows/fileformat/allplayer_m3u_bof	2013-10-09	normal	This module exploits a stack-based buffer overflow vulnerability in ALLPlayer 5.8.1, caused by a long string in a playlist entry. E persuading the victim to open a specially-c .M3U file, a ... **Platforms**: win **CVEs**: CVE-2013-7409 **Refs**: source, ref1
Altap Salamander 2.5 PE Viewer Buffer Overflow exploit/windows/fileformat/altap_salamander_pdb	2007-06-19	good	This module exploits a buffer overflow in A Salamander <= v2.5. By creating a malicio and convincing a user to view the file with t Portable Executable Viewer plugin within a vulnerable ... **Platforms**: win **CVEs**: CVE-2007-3314 **Refs**: source, ref1
AOL Desktop 9.6 RTX Buffer Overflow exploit/windows/fileformat/aol_desktop_linktag	2011-01-31	normal	This module exploits a vulnerability found i AOL Desktop 9.6's Toolrich.rct component. supplying a long string of data in the hyper tag, rich.rct copies this data into a buffer us strcpy ... **Platforms**: win **Refs**: source
AOL 9.5 Phobos.Playlist Import() Stack-based Buffer Overflow exploit/windows/fileformat/aol_phobos_bof	2010-01-20	average	This module exploits a stack-based buffer overflow within Phobos.dll of AOL 9.5. By setting an overly long value to 'Import()', ar attacker can overrun a buffer and execute arbitrary code. NOTE: This ... **Platforms**: win **Refs**: source, ref1
Apple QuickTime PICT PnSize Buffer Overflow exploit/windows/fileformat/apple_quicktime_pnsize	2011-08-08	good	This module exploits a vulnerability in Appl QuickTime Player 7.60.92.0. When openin .mov file containing a specially crafted PnS value, an attacker may be able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2011-0257 **Refs**: source
Apple Quicktime 7 Invalid Atom Length Buffer Overflow exploit/windows/fileformat/apple_quicktime_rdrf	2013-05-22	normal	This module exploits a vulnerability found i Apple QuickTime. The flaw is triggered wh QuickTime fails to properly handle the data length for certain atoms such as 'rdrf' or 'dr the Alis ... **Platforms**: win **CVEs**: CVE-2013-1017 **Refs**: source, ref1
Apple QuickTime TeXML Style Element Stack Buffer Overflow exploit/windows/fileformat/apple_quicktime_texml	2012-05-15	normal	This module exploits a vulnerability found i Apple QuickTime. When handling a TeXML it is possible to trigger a stack-based buffe overflow, and then gain arbitrary code exec under the ... **Platforms**: win **CVEs**: CVE-2012-0663, CVE-2012-0664 **Refs**: source, ref1, ref2
Audiotran 1.4.1 (PLS File) Stack Buffer Overflow exploit/windows/fileformat/audiotran_pls	2010-01-09	good	This module exploits a stack-based buffer overflow in Audiotran 1.4.1. An attacker mu send the file to victim and the victim must c the file. Alternatively it may be possible to execute code ... **Platforms**: win **CVEs**: CVE-2009-0476 **Refs**: source

Metasploit Module	Date	Rank	Details
Audiotran PLS File Stack Buffer Overflow exploit/windows/fileformat/audiotran_pls_1424	2010-09-09	good	This module exploits a stack-based buffer overflow in Audiotran 1.4.2.4. An attacker r send the file to victim and the victim must c the file. Alternatively, it may be possible to execute code ... **Platforms**: win **Refs**: source
AudioCoder .M3U Buffer Overflow exploit/windows/fileformat/audio_coder_m3u	2013-05-01	normal	This module exploits a buffer overflow in AudioCoder 0.8.18. The vulnerability occur when adding an .m3u, allowing arbitrary cc execution with the privileges of the user ru AudioCoder. This ... **Platforms**: win **CVEs**: CVE-2017-8870 **Refs**: source
Audio Workstation 6.4.2.4.3 pls Buffer Overflow exploit/windows/fileformat/audio_wkstn_pls	2009-12-08	good	This module exploits a buffer overflow in A Workstation 6.4.2.4.3. When opening a malicious pls file with the Audio Workstatio remote attacker could overflow a buffer an execute arbitrary ... **Platforms**: win **CVEs**: CVE-2009-0476 **Refs**: source
A-PDF WAV to MP3 v1.0.0 Buffer Overflow exploit/windows/fileformat/a_pdf_wav_to_mp3	2010-08-17	normal	This module exploits a buffer overflow in A WAV to MP3 v1.0.0. When the application used to import a specially crafted m3u file, buffer overflow occurs allowing arbitrary co execution. **Platforms**: win **Refs**: source
BACnet OPC Client Buffer Overflow exploit/windows/fileformat/bacnet_csv	2010-09-16	good	This module exploits a stack buffer overflo SCADA Engine BACnet OPC Client v1.0.2 When the BACnet OPC Client parses a specially crafted csv file, arbitrary code ma executed. **Platforms**: win **CVEs**: CVE-2010-4740 **Refs**: source, ref1
Beetel Connection Manager NetConfig.ini Buffer Overflow exploit/windows/fileformat/beetel_netconfig_ini_bof	-	normal	This module exploits a stack-based buffer overflow in Beetel Connection Manager. Th vulnerability exists in the parsing of the UserName parameter in the NetConfig.ini f The module has been ... **Platforms**: win **Refs**: source
BlazeVideo HDTV Player Pro v6.6 Filename Handling Vulnerability exploit/windows/fileformat/blazedvd_hdtv_bof	2012-04-03	normal	This module exploits a vulnerability found i BlazeVideo HDTV Player's filename handli routine. When supplying a string of input da embedded in a .plf file, the MediaPlayerCtr component will ... **Platforms**: win **Refs**: source
BlazeDVD 6.1 PLF Buffer Overflow exploit/windows/fileformat/blazedvd_plf	2009-08-03	good	This module exploits a stack over flow in BlazeDVD 5.1 and 6.2. When the applicati used to open a specially crafted plf file, a b is overwritten allowing for the execution of arbitrary code. **Platforms**: win **CVEs**: CVE-2006-6199 **Refs**: source
Boxoft WAV to MP3 Converter v1.1 Buffer Overflow exploit/windows/fileformat/boxoft_wav_to_mp3	2015-08-31	normal	This module exploits a stack buffer overflo Boxoft WAV to MP3 Converter versions 1.0 1.1. By constructing a specially crafted WA and attempting to convert it to an MP3 file ... **Platforms**: win **CVEs**: CVE-2015-7243 **Refs**: source

Metasploit Module	Date	Rank	Details
BulletProof FTP Client BPS Buffer Overflow exploit/windows/fileformat/bpftp_client_bps_bof	2014-07-24	normal	This module exploits a stack-based buffer overflow vulnerability in BulletProof FTP Cl 2010, caused by an overly long hostname. persuading the victim to open a specially-c .BPS file, a ... **Platforms**: win **CVEs**: CVE-2014-2973 **Refs**: source
BS.Player 2.57 Buffer Overflow (Unicode SEH) exploit/windows/fileformat/bsplayer_m3u	2010-01-07	normal	This module exploits a buffer overflow in BS.Player 2.57. When the playlist import is to import a specially crafted m3u file, a buf overflow occurs allowing arbitrary code execution. **Platforms**: win **Refs**: source
Cain and Abel RDP Buffer Overflow exploit/windows/fileformat/cain_abel_4918_rdp	2008-11-30	good	This module exploits a stack-based buffer overflow in the Cain Abel v4.9.24 and belo attacker must send the file to victim, and th victim must open the specially crafted RDF under Tools ... **Platforms**: win **CVEs**: CVE-2008-5405 **Refs**: source
CA Antivirus Engine CAB Buffer Overflow exploit/windows/fileformat/ca_cab	2007-06-05	good	This module exploits a stack buffer overflo CA eTrust Antivirus 8.1.637. By creating a specially crafted CAB file, an attacker may able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2007-2864 **Refs**: source
CCMPlayer 1.5 m3u Playlist Stack Based Buffer Overflow exploit/windows/fileformat/ccmplayer_m3u_bof	2011-11-30	good	This module exploits a stack based buffer overflow in CCMPlayer 1.5. Opening a m3 playlist with a long track name, a SEH exce record can be overwritten with parts of the controllable buffer. ... **Platforms**: win **CVEs**: CVE-2011-5170 **Refs**: source
Chasys Draw IES Buffer Overflow exploit/windows/fileformat/chasys_draw_ies_bmp_bof	2013-07-26	normal	This module exploits a buffer overflow vulnerability found in Chasys Draw IES (ve 4.10.01). The vulnerability exists in the mo flt_BMP.dll, while parsing BMP files, where ReadFile ... **Platforms**: win **CVEs**: CVE-2013-3928 **Refs**: source, ref1, ref2
Cool PDF Image Stream Buffer Overflow exploit/windows/fileformat/coolpdf_image_stream_bof	2013-01-18	normal	This module exploits a stack buffer overflo Cool PDF Reader prior to version 3.0.2.25 The vulnerability is triggered when openinc malformed PDF file that contains a special crafted image ... **Platforms**: win **CVEs**: CVE-2012-4914 **Refs**: source, ref1
Corel PDF Fusion Stack Buffer Overflow exploit/windows/fileformat/corelpdf_fusion_bof	2013-07-08	normal	This module exploits a stack-based buffer overflow vulnerability in version 1.11 of Co PDF Fusion. The vulnerability exists while handling a XPS file with long entry names. order for the ... **Platforms**: win **CVEs**: CVE-2013-3248 **Refs**: source, ref1
Csound hetro File Handling Stack Buffer Overflow exploit/windows/fileformat/csound_getnum_bof	2012-02-23	normal	This module exploits a buffer overflow in Csound before 5.16.6. The overflow occurs when trying to import a malicious hetro file tabular format. In order to achieve exploita the user should ... **Platforms**: win **CVEs**: CVE-2012-0270 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
LNK Code Execution Vulnerability exploit/windows/fileformat/cve_2017_8464_lnk_rce	2017-06-13	excellent	This module exploits a vulnerability in the handling of Windows Shortcut files (.LNK) f contain a dynamic icon, loaded from a mal DLL. This vulnerability is a variant of MS15 ... **Platforms**: win **CVEs**: CVE-2015-0096, CVE-2017-8464 **Refs**: source, ref1, ref2, ref3, ref4, ref5
CyberLink LabelPrint 2.5 Stack Buffer Overflow exploit/windows/fileformat/cyberlink_lpp_bof	2017-09-23	normal	This module exploits a stack buffer overflo CyberLink LabelPrint 2.5 and below. The vulnerability is triggered when opening a .lp project file containing overly long string characters via open ... **Platforms**: win **CVEs**: CVE-2017-14627 **Refs**: source
CyberLink Power2Go name Attribute (p2g) Stack Buffer Overflow Exploit exploit/windows/fileformat/cyberlink_p2g_bof	2011-09-12	great	This module exploits a stack buffer overflo CyberLink Power2Go version 8.x The vulnerability is triggered when opening a malformed p2g file containing an overly lor string in the 'name' ... **Platforms**: win **CVEs**: CVE-2011-5171 **Refs**: source
Cytel Studio 9.0 (CY3 File) Stack Buffer Overflow exploit/windows/fileformat/cytel_studio_cy3	2011-10-02	good	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. **Platforms**: win **Refs**: source, ref1
AstonSoft DeepBurner (DBR File) Path Buffer Overflow exploit/windows/fileformat/deepburner_path	2006-12-19	great	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 mu send the file to victim and ... **Platforms**: win **CVEs**: CVE-2006-6665 **Refs**: source
Destiny Media Player 1.61 PLS M3U Buffer Overflow exploit/windows/fileformat/destinymediaplayer16	2009-01-03	good	This module exploits a stack-based buffer overflow in the Destiny Media Player 1.61. attacker must send the file to victim and the victim must open the file. File-->Open Play **Platforms**: win **CVEs**: CVE-2009-3429 **Refs**: source
Digital Music Pad Version 8.2.3.3.4 Stack Buffer Overflow exploit/windows/fileformat/digital_music_pad_pls	2010-09-17	normal	This module exploits a buffer overflow in D Music Pad Version 8.2.3.3.4 When opening malicious pls file with the Digital Music Pad remote attacker could overflow a buffer and execute ... **Platforms**: win **Refs**: source, ref1
DJ Studio Pro 5.1 .pls Stack Buffer Overflow exploit/windows/fileformat/djstudio_pls_bof	2009-12-30	normal	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 supplied data on the stack without any prop bounds checking ... **Platforms**: win **CVEs**: CVE-2009-4656 **Refs**: source
DjVu DjVu_ActiveX_MSOffice.dll ActiveX ComponentBuffer Overflow exploit/windows/fileformat/djvu_imageurl	2008-10-30	low	This module exploits a stack buffer overflo DjVu ActiveX Component. When sending a overly long string to the ImageURL() prope DjVu_ActiveX_MSOffice.dll (3.0) an attacke may be able to ... **Platforms**: win **CVEs**: CVE-2008-4922 **Refs**: source

Metasploit Module	Date	Rank	Details
Documalis Free PDF Editor and Scanner JPEG Stack Buffer Overflow exploit/windows/fileformat/documalis_pdf_editor_and_scanner	2020-05-22	normal	Documalis Free PDF Editor version 5.7.2.2 and Documalis Free PDF Scanner version 5.7.2.122 do not appropriately validate the contents of JPEG images contained within PDF. Attackers can exploit ... **Platforms**: win **Refs**: source
Dup Scout Enterprise v10.4.16 - Import Command Buffer Overflow exploit/windows/fileformat/dupscout_xml	2017-03-29	normal	This module exploits a buffer overflow in D Scout Enterprise v10.4.16 by using the imp command option to import a specially craft xml file. **Platforms**: win **CVEs**: CVE-2017-7310 **Refs**: source
DVD X Player 5.5 .plf PlayList Buffer Overflow exploit/windows/fileformat/dvdx_plf_bof	2007-06-02	normal	This module exploits a stack-based buffer overflow on DVD X Player 5.5 Pro and Standard. By supplying a long string of dat plf file (playlist), the MediaPlayerCtrl.dll component will attempt to ... **Platforms**: win **CVEs**: CVE-2007-3068 **Refs**: source
Easy CD-DA Recorder PLS Buffer Overflow exploit/windows/fileformat/easycdda_pls_bof	2010-06-07	normal	This module exploits a stack-based buffer overflow vulnerability in Easy CD-DA Reco 2007 caused by an overlong string in a pla entry. By persuading the victim to open a specially-crafted PLS ... **Platforms**: win **CVEs**: CVE-2010-2343 **Refs**: source, ref1
EMC ApplicationXtender (KeyWorks) ActiveX Control Buffer Overflow exploit/windows/fileformat/emc_appextender_keyworks	2009-09-29	average	This module exploits a stack buffer overflo the KeyWorks KeyHelp ActiveX Control (KeyHelp.ocx 1.2.3120.0). This ActiveX Co comes bundled with EMC's Documentatior ApplicationXtender 5.4. **Platforms**: win **CVEs**: CVE-2012-2515 **Refs**: source
ERS Viewer 2011 ERS File Handling Buffer Overflow exploit/windows/fileformat/erdas_er_viewer_bof	2013-04-23	normal	This module exploits a buffer overflow vulnerability found in ERS Viewer 2011 (ve 11.04). The vulnerability exists in the modu ermapper_u.dll where the function ERM_convert_to_correct_webpath ... **Platforms**: win **CVEs**: CVE-2013-0726 **Refs**: source, ref1
Adobe PDF Embedded EXE Social Engineering exploit/windows/fileformat/adobe_pdf_embedded_exe	2010-03-29	excellent	This module embeds a Metasploit payload an existing PDF file. The resulting PDF car sent to a target as part of a social engineer attack. **Platforms**: win **CVEs**: CVE-2010-1240 **Refs**: source, ref1, ref2, ref3, ref4
Aviosoft Digital TV Player Professional 1.0 Stack Buffer Overflow exploit/windows/fileformat/aviosoft_plf_buf	2011-11-09	good	This module exploits a vulnerability found i Aviosoft Digital TV Player Pro version 1.x. overflow occurs when the process copies t content of a playlist file on to the stack, wh may result ... **Platforms**: win **Refs**: source
GlobalSCAPE CuteZIP Stack Buffer Overflow exploit/windows/fileformat/cutezip_bof	2011-02-12	normal	This module exploits a stack-based buffer overflow vulnerability in version 2.1 of Cute In order for the command to be executed, a attacker must convince the target user to o specially ... **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
ERS Viewer 2013 ERS File Handling Buffer Overflow exploit/windows/fileformat/erdas_er_viewer_rf_report_error	-	normal	This module exploits a buffer overflow vulnerability found in ERS Viewer 2013. Th vulnerability exists in the module ermapper_u.dll, where the function rf_report_error handles user provided data **Platforms**: win **CVEs**: CVE-2013-3482 **Refs**: source, ref1
HTML Help Workshop 4.74 (hhp Project File) Buffer Overflow exploit/windows/fileformat/hhw_hhp_contentfile_bof	2006-02-06	good	This module exploits a stack buffer overflo HTML Help Workshop 4.74 by creating a specially crafted hhp file. **Platforms**: win **CVEs**: CVE-2006-0564 **Refs**: source
McAfee SaaS MyCioScan ShowReport Remote Command Execution exploit/windows/fileformat/mcafee_showreport_exec	2012-01-12	normal	This module exploits a vulnerability found i McAfee Security-as-a-Service. The ShowReport() function (located in the myCIOScn.dll ActiveX component) fails to the FileName argument, and passes ... **Platforms**: win **Refs**: source
MS11-006 Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow exploit/windows/fileformat/ms11_006_createsizeddibsection	2010-12-15	great	This module exploits a stack-based buffer overflow in the handling of thumbnails with .MIC files and various Office documents. W processing a thumbnail bitmap containing a negative 'biClrUsed' ... **Platforms**: win **CVEs**: CVE-2010-3970 **Refs**: source
Nitro Pro PDF Reader 11.0.3.173 Javascript API Remote Code Execution exploit/windows/fileformat/nitro_reader_jsapi	2017-07-24	excellent	This module exploits an unsafe Javascript implemented in Nitro and Nitro Pro PDF Re version 11. The saveAs() Javascript API function allows for writing arbitrary files to t file system. ... **Platforms**: win **CVEs**: CVE-2017-7442 **Refs**: source, ref1, ref2
RealPlayer RealMedia File Handling Buffer Overflow exploit/windows/fileformat/real_player_url_property_bof	2012-12-14	normal	This module exploits a stack based buffer overflow on RealPlayer <=15.0.6.14. The vulnerability exists in the handling of real m files, due to the insecure usage of the GetPrivateProfileString ... **Platforms**: win **CVEs**: CVE-2012-5691 **Refs**: source, ref1
VideoLAN VLC TiVo Buffer Overflow exploit/windows/fileformat/videolan_tivo	2008-10-22	good	This module exploits a buffer overflow in VideoLAN VLC 0.9.4. By creating a malicic TY file, a remote attacker could overflow a buffer and execute arbitrary code. **Platforms**: win **CVEs**: CVE-2008-4654 **Refs**: source
eSignal and eSignal Pro File Parsing Buffer Overflow in QUO exploit/windows/fileformat/esignal_styletemplate_bof	2011-09-06	normal	The software is unable to handle the "" files (even those original included in the prograr like those with the registered extensions Q SUM and POR. Successful exploitation of t **Platforms**: win **CVEs**: CVE-2011-3494 **Refs**: source, ref1
CA eTrust PestPatrol ActiveX Control Buffer Overflow exploit/windows/fileformat/etrust_pestscan	2009-11-02	average	This module exploits a stack buffer overflo CA eTrust PestPatrol. When sending an ov long string to the Initialize() property of ppc (5.6.7.9) an attacker may be able to execut **Platforms**: win **CVEs**: CVE-2009-4225 **Refs**: source

Metasploit Module	Date	Rank	Details
eZip Wizard 3.0 Stack Buffer Overflow exploit/windows/fileformat/ezip_wizard_bof	2009-03-09	good	This module exploits a stack-based buffer overflow vulnerability in version 3.0 of ediS Corp.'s eZip Wizard. In order for the comm to be executed, an attacker must convince someone to open a ... **Platforms**: win **CVEs**: CVE-2009-1028 **Refs**: source, ref1
Fat Player Media Player 0.6b0 Buffer Overflow exploit/windows/fileformat/fatplayer_wav	2010-10-18	normal	This module exploits a buffer overflow in F Player 0.6b. When the application is used t import a specially crafted wav file, a buffer overflow occurs allowing arbitrary code execution. **Platforms**: win **CVEs**: CVE-2009-4962 **Refs**: source
Free Download Manager Torrent Parsing Buffer Overflow exploit/windows/fileformat/fdm_torrent	2009-02-02	good	This module exploits a stack buffer overflo Free Download Manager 3.0 Build 844. Arbitrary code execution could occur when parsing a specially crafted torrent file. **Platforms**: win **CVEs**: CVE-2009-0184 **Refs**: source, ref1, ref2, ref3, ref4
FeedDemon Stack Buffer Overflow exploit/windows/fileformat/feeddemon_opml	2009-02-09	great	This module exploits a buffer overflow in FeedDemon v3.1.0.12. When the applicati used to import a specially crafted opml file, buffer overflow occurs allowing arbitrary co execution. All ... **Platforms**: win **CVEs**: CVE-2009-0546 **Refs**: source
Foxit PDF Reader 4.2 Javascript File Write exploit/windows/fileformat/foxit_reader_filewrite	2011-03-05	normal	This module exploits an unsafe Javascript implemented in Foxit PDF Reader version The createDataObject() Javascript API fun allows for writing arbitrary files to the file system. This ... **Platforms**: win **Refs**: source, ref1
Foxit Reader 3.0 Open Execute Action Stack Based Buffer Overflow exploit/windows/fileformat/foxit_reader_launch	2009-03-09	good	This module exploits a buffer overflow in F Reader 3.0 builds 1301 and earlier. Due to way Foxit Reader handles the input from a "Launch" action, it is possible to cause a st based buffer ... **Platforms**: win **CVEs**: CVE-2009-0837 **Refs**: source, ref1
Foxit PDF Reader Pointer Overwrite UAF exploit/windows/fileformat/foxit_reader_uaf	2018-04-20	normal	Foxit PDF Reader v9.0.1.1049 has a Use-A Free vulnerability in the Text Annotations component and the TypedArray's use uninitialized pointers. The vulnerabilities ca combined to leak a vtable ... **Platforms**: win **CVEs**: CVE-2018-99, CVE-2018-9948, CV 2018-9958 **Refs**: source, ref1, ref2
Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow exploit/windows/fileformat/foxit_title_bof	2010-11-13	great	This module exploits a stack buffer overflo Foxit PDF Reader prior to version 4.2.0.09 The vulnerability is triggered when openinc malformed PDF file that contains an overly string in ... **Platforms**: win **Refs**: source, ref1
Free MP3 CD Ripper 1.1 WAV File Stack Buffer Overflow exploit/windows/fileformat/free_mp3_ripper_wav	2011-08-27	great	This module exploits a stack based buffer overflow found in Free MP3 CD Ripper 1.1 overflow is triggered when an unsuspectinc opens a malicious WAV file. **Platforms**: win **CVEs**: CVE-2011-5165 **Refs**: source

Metasploit Module	Date	Rank	Details
gAlan 0.2.1 Buffer Overflow exploit/windows/fileformat/galan_fileformat_bof	2009-12-07	normal	This module exploits a stack buffer overflo gAlan 0.2.1 by creating a specially crafted file. **Platforms**: win **Refs**: source
GSM SIM Editor 5.15 Buffer Overflow exploit/windows/fileformat/gsm_sim	2010-07-07	normal	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 o which allows an attacker ... **Platforms**: win **CVEs**: CVE-2015-1171 **Refs**: source
GTA SA-MP server.cfg Buffer Overflow exploit/windows/fileformat/gta_samp	2011-09-18	normal	This module exploits a stack-based buffer overflow in GTA SA-MP Server. This buffer overflow occurs when the application atten to open a malformed server.cfg file. To exp this vulnerability, ... **Platforms**: win **Refs**: source
HTML Help Workshop 4.74 (hhp Project File) Buffer Overflow exploit/windows/fileformat/hhw_hhp_compiledfile_bof	2006-02-06	good	This module exploits a stack buffer overflo HTML Help Workshop 4.74 By creating a specially crafted hhp file, an attacker may b able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2006-0564 **Refs**: source
HTML Help Workshop 4.74 (hhp Project File) Buffer Overflow exploit/windows/fileformat/hhw_hhp_indexfile_bof	2009-01-17	good	This module exploits a stack buffer overflo HTML Help Workshop 4.74 by creating a specially crafted hhp file. **Platforms**: win **CVEs**: CVE-2009-0133 **Refs**: source
Heroes of Might and Magic III .h3m Map file Buffer Overflow exploit/windows/fileformat/homm3_h3m	2015-07-29	normal	This module embeds an exploit into an uncompressed map file (.h3m) for Heroes Might and Magic III. Once the map is starte game, a buffer overflow occurring when loa object sprite names ... **Platforms**: win **Refs**: source
HT-MP3Player 1.0 HT3 File Parsing Buffer Overflow exploit/windows/fileformat/ht_mp3player_ht3_bof	2009-06-29	good	This module exploits a stack buffer overflo HT-MP3Player 1.0. Arbitrary code executio could occur when parsing a specially crafte .HT3 file. NOTE: The player installation do not register the ... **Platforms**: win **CVEs**: CVE-2009-2485 **Refs**: source
IBM Forms Viewer Unicode Buffer Overflow exploit/windows/fileformat/ibm_forms_viewer_fontname	2013-12-05	normal	This module exploits a stack-based buffer overflow in IBM Forms Viewer. The vulnera is due to a dangerous usage of a strcpy-lik function, and occurs while parsing malform XFDL files ... **Platforms**: win **CVEs**: CVE-2013-5447 **Refs**: source, ref1
IBM Personal Communications iSeries Access WorkStation 5.9 Profile exploit/windows/fileformat/ibm_pcm_ws	2012-02-28	great	The IBM Personal Communications I-Serie application WorkStation is susceptible to a stack-based buffer overflow vulnerability w file parsing in which data copied to a locati memory exceeds ... **Platforms**: win **CVEs**: CVE-2012-0201 **Refs**: source, ref1
IcoFX Stack Buffer Overflow exploit/windows/fileformat/icofx_bof	2013-12-10	normal	This module exploits a stack-based buffer overflow vulnerability in version 2.1 of IcoF The vulnerability exists while parsing .ICO where a specially crafted ICONDIR header providing an ... **Platforms**: win **CVEs**: CVE-2013-4988 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
PointDev IDEAL Migration Buffer Overflow exploit/windows/fileformat/ideal_migration_ipj	2009-12-05	great	This module exploits a stack buffer overflo versions v9.7 through v10.5 of IDEAL Administration and versions 4.5 and 4.51 c IDEAL Migration. All versions are suspecte be vulnerable. By ... **Platforms**: win **CVEs**: CVE-2009-4265 **Refs**: source
i-FTP Schedule Buffer Overflow exploit/windows/fileformat/iftp_schedule_bof	2014-11-06	normal	This module exploits a stack-based buffer overflow vulnerability in i-Ftp v2.20, caused long time value set for scheduled downloa persuading the victim to place a specially-crafted ... **Platforms**: win **Refs**: source
Irfanview JPEG2000 jp2 Stack Buffer Overflow exploit/windows/fileformat/irfanview_jpeg2000_bof	2012-01-16	normal	This module exploits a stack-based buffer overflow vulnerability in version <= 4.3.2.0 Irfanview's JPEG2000.dll plugin. This explo has been tested on a specific version of irfanview (v4.3.2), ... **Platforms**: win **CVEs**: CVE-2012-0897 **Refs**: source, ref1
Lattice Semiconductor ispVM System XCF File Handling Overflow exploit/windows/fileformat/ispvm_xcf_ispxcf	2012-05-16	normal	This module exploits a vulnerability found i ispVM System 18.0.2. Due to the way ispV handles .xcf files, it is possible to cause a b overflow with a specially crafted file, when long value ... **Platforms**: win **Refs**: source, ref1
KingView Log File Parsing Buffer Overflow exploit/windows/fileformat/kingview_kingmess_kvl	2012-11-20	normal	This module exploits a vulnerability found i KingView <= 6.55. It exists in the KingMess application when handling log files, due to insecure usage of sprintf. This module use malformed ... **Platforms**: win **CVEs**: CVE-2012-4711 **Refs**: source, ref1
Lattice Semiconductor PAC-Designer 6.21 Symbol Value Buffer Overflow exploit/windows/fileformat/lattice_pac_bof	2012-05-16	normal	This module exploits a vulnerability found i Lattice Semiconductor PAC-Designer 6.21 .pac file, when supplying a long string of da the 'value' field under the 'SymbolicSchematicData' tag, ... **Platforms**: win **CVEs**: CVE-2012-2915 **Refs**: source, ref1
Lotus Notes 8.0.x - 8.5.2 FP2 - Autonomy Keyview (.lzh Attachment) exploit/windows/fileformat/lotusnotes_lzh	2011-05-24	good	This module exploits a stack buffer overflo Lotus Notes 8.5.2 when parsing a malform specially crafted LZH file. This vulnerability discovered binaryhouse.net. **Platforms**: win **CVEs**: CVE-2011-1213 **Refs**: source, ref1, ref2
Magix Musik Maker 16 .mmm Stack Buffer Overflow exploit/windows/fileformat/magix_musikmaker_16_mmm	2011-04-26	good	This module exploits a stack buffer overflo Magix Musik Maker 16. When opening a specially crafted arrangement file (.mmm) i application, an unsafe strcpy() will allow yo overwrite a SEH ... **Platforms**: win **Refs**: source, ref1
McAfee Remediation Client ActiveX Control Buffer Overflow exploit/windows/fileformat/mcafee_hercules_deletesnapshot	2008-08-04	low	This module exploits a stack buffer overflo McAfee Remediation Agent 4.5.0.41. Wher sending an overly long string to the DeleteSnapshot() method of enginecom.dl (3.7.0.9) an attacker may be able ... **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
MediaCoder .M3U Buffer Overflow exploit/windows/fileformat/mediacoder_m3u	2013-06-24	normal	This module exploits a buffer overflow in MediaCoder 0.8.22. The vulnerability occu when adding an .m3u, allowing arbitrary cc execution under the context of the user. DE bypass via ROP is ... **Platforms**: win **CVEs**: CVE-2017-8869 **Refs**: source
Media Jukebox 8.0.400 Buffer Overflow (SEH) exploit/windows/fileformat/mediajukebox	2009-07-01	normal	This module exploits a stack buffer overflo Media Jukebox 8.0.400 by creating a spec crafted m3u or pls file. **Platforms**: win **CVEs**: CVE-2009-2650 **Refs**: source
MicroP 0.1.1.1600 (MPPL File) Stack Buffer Overflow exploit/windows/fileformat/microp_mppl	2010-08-23	great	This module exploits a vulnerability found i MicroP 0.1.1.1600. A stack-based buffer overflow occurs when the content of a .mp gets copied onto the stack, which overwrite lpFileName ... **Platforms**: win **CVEs**: CVE-2010-5299 **Refs**: source
Microsoft Windows Contact File Format Arbitary Code Execution exploit/windows/fileformat/microsoft_windows_contact	2019-01-17	normal	This vulnerability allows remote attackers t execute arbitrary code on vulnerable installations of Microsoft Windows. User interaction is required to exploit this vulnera in that the target ... **Platforms**: win **Refs**: source, ref1
Millenium MP3 Studio 2.0 (PLS File) Stack Buffer Overflow exploit/windows/fileformat/millenium_mp3_pls	2009-07-30	great	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 ma possible to execute ... **Platforms**: win **Refs**: source
Mini-Stream RM-MP3 Converter v3.1.2.1 PLS File Stack Buffer Overflow exploit/windows/fileformat/mini_stream_pls_bof	2010-07-16	great	This module exploits a stack based buffer overflow found in Mini-Stream RM-MP3 Converter v3.1.2.1. The overflow is triggere when an unsuspecting victim opens the malicious PLS file. **Platforms**: win **CVEs**: CVE-2010-5081 **Refs**: source
MJM Core Player 2011 .s3m Stack Buffer Overflow exploit/windows/fileformat/mjm_coreplayer2011_s3m	2011-04-30	good	This module exploits a stack buffer overflo MJM Core Player 2011 When opening a malicious s3m file in this application, a stac buffer overflow can be triggered, resulting i arbitrary code ... **Platforms**: win **Refs**: source, ref1
MJM QuickPlayer 1.00 Beta 60a / QuickPlayer 2010 .s3m Stack Buffer Overflow exploit/windows/fileformat/mjm_quickplayer_s3m	2011-04-30	good	This module exploits a stack buffer overflo MJM QuickPlayer 1.00 beta 60a and QuickPlayer 2010 (Multi-target exploit). Wh opening a malicious s3m file in one of thes applications, a stack ... **Platforms**: win **Refs**: source, ref1
MOXA MediaDBPlayback ActiveX Control Buffer Overflow exploit/windows/fileformat/moxa_mediadbplayback	2010-10-19	average	This module exploits a stack buffer overflo MOXA_ActiveX_SDK. When sending an ov long string to the PlayFileName() of MediaDBPlayback.DLL (2.2.0.5) an attacke may be able to execute ... **Platforms**: win **CVEs**: CVE-2010-4742 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
MPlayer Lite M3U Buffer Overflow exploit/windows/fileformat/mplayer_m3u_bof	2011-03-19	average	This module exploits a stack-based buffer overflow vulnerability in MPlayer Lite r3306 caused by improper bounds checking of ar entry. By persuading the victim to open a specially-crafted .M3U ... **Platforms**: win **Refs**: source, ref1
MPlayer SAMI Subtitle File Buffer Overflow exploit/windows/fileformat/mplayer_sami_bof	2011-05-19	normal	This module exploits a stack-based buffer overflow found in the handling of SAMI sub files in MPlayer SVN Versions before 3347 currently targets SMPlayer 0.6.8, which is distributed with a ... **Platforms**: win **Refs**: source, ref1
MS09-067 Microsoft Excel Malformed FEATHEADER Record Vulnerability exploit/windows/fileformat/ms09_067_excel_featheader	2009-11-10	good	This module exploits a vulnerability in the handling of the FEATHEADER record by Microsoft Excel. Revisions of Office XP an prior to the release of the MS09-067 bulleti vulnerable. When ... **Platforms**: win **CVEs**: CVE-2009-3129 **Refs**: source, ref1
MS10-004 Microsoft PowerPoint Viewer TextBytesAtom Stack Buffer Overflow exploit/windows/fileformat/ms10_004_textbytesatom	2010-02-09	good	This module exploits a stack buffer overflo vulnerability in the handling of the TextBytesAtom records by Microsoft Powe Viewer. According to Microsoft, the PowerF Viewer distributed with ... **Platforms**: win **CVEs**: CVE-2010-0033 **Refs**: source
MS11-038 Microsoft Office Excel Malformed OBJ Record Handling Overflow exploit/windows/fileformat/ms10_038_excel_obj_bof	2010-06-08	normal	This module exploits a vulnerability found i Excel 2002 of Microsoft Office XP. By supp a .xls file with a malformed OBJ (recType record an attacker can get the control of th execution ... **Platforms**: win **CVEs**: CVE-2010-0822 **Refs**: source, ref1
MS10-087 Microsoft Word RTF pFragments Stack Buffer Overflow (File Format) exploit/windows/fileformat/ms10_087_rtf_pfragments_bof	2010-11-09	great	This module exploits a stack-based buffer overflow in the handling of the 'pFragments shape property within the Microsoft Word F parser. All versions of Microsoft Office 201 2007, 2003, and XP ... **Platforms**: win **CVEs**: CVE-2010-3333 **Refs**: source, ref1
MS11-021 Microsoft Office 2007 Excel .xlb Buffer Overflow exploit/windows/fileformat/ms11_021_xlb_bof	2011-08-09	normal	This module exploits a vulnerability found i Excel of Microsoft Office 2007. By supplyin malformed .xlb file, an attacker can control content (source) of a memcpy routine, and number of ... **Platforms**: win **CVEs**: CVE-2011-0105 **Refs**: source
MS12-005 Microsoft Office ClickOnce Unsafe Object Package Handling Vulnerability exploit/windows/fileformat/ms12_005	2012-01-10	excellent	This module exploits a vulnerability found i Microsoft Office's ClickOnce feature. Wher handling a Macro document, the applicatio to recognize certain file extensions as dangerous ... **Platforms**: win **CVEs**: CVE-2012-0013 **Refs**: source, ref1, ref2
MS12-027 MSCOMCTL ActiveX Buffer Overflow exploit/windows/fileformat/ms12_027_mscomctl_bof	2012-04-10	average	This module exploits a stack buffer overflo MSCOMCTL.OCX. It uses a malicious RTF embed the specially crafted MSComctlLib.ListViewCtrl.2 Control as exp in the wild on April 2012. This ... **Platforms**: win **CVEs**: CVE-2012-0158 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution exploit/windows/fileformat/ms13_071_theme	2013-09-10	excellent	This module exploits a vulnerability mainly affecting Microsoft Windows XP and Windc 2003. The vulnerability exists in the handlir the Screen Saver path, in the [boot] sectior arbitrary ... **Platforms**: win **CVEs**: CVE-2013-0810 **Refs**: source, ref1, ref2
MS14-017 Microsoft Word RTF Object Confusion exploit/windows/fileformat/ms14_017_rtf	2014-04-01	normal	This module creates a malicious RTF file th when opened in vulnerable versions of Mic Word will lead to code execution. The flaw exists in how a listoverridecount field can b modified to ... **Platforms**: win **CVEs**: CVE-2014-1761 **Refs**: source, ref1, ref2
MS14-060 Microsoft Windows OLE Package Manager Code Execution exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	This module exploits a vulnerability found i Windows Object Linking and Embedding ((allowing arbitrary code execution, publicly known as "Sandworm". Platforms such as Windows Vista SP2 all the ... **Platforms**: win **CVEs**: CVE-2014-4114 **Refs**: source, ref1, ref2
MS14-064 Microsoft Windows OLE Package Manager Code Execution Through Python exploit/windows/fileformat/ms14_064_packager_python	2014-11-12	excellent	This module exploits a vulnerability found i Windows Object Linking and Embedding ((allowing arbitrary code execution, bypassir patch MS14-060, for the vulnerability publi known as ... **Platforms**: python **CVEs**: CVE-2014-4114, CVE-2014-6352 **Refs**: source, ref1
MS14-064 Microsoft Windows OLE Package Manager Code Execution exploit/windows/fileformat/ms14_064_packager_run_as_admin	2014-10-21	excellent	This module exploits a vulnerability found i Windows Object Linking and Embedding ((allowing arbitrary code execution, publicly exploited in the wild as MS14-060 patch by The Microsoft ... **Platforms**: win **CVEs**: CVE-2014-6352 **Refs**: source, ref1
Microsoft Windows Shell LNK Code Execution exploit/windows/fileformat/ms15_020_shortcut_icon_dllloader	2015-03-10	excellent	This module exploits a vulnerability in the MS10-046 patch to abuse (again) the hanc of Windows Shortcut files (.LNK) that conta icon resource pointing to a malicious DLL. module ... **Platforms**: win **CVEs**: CVE-2015-0096 **Refs**: source, ref1, ref2
MS15-100 Microsoft Windows Media Center MCL Vulnerability exploit/windows/fileformat/ms15_100_mcl_exe	2015-09-08	excellent	This module exploits a vulnerability in Winc Media Center. By supplying an UNC path i *.mcl file, a remote file will be automatically downloaded, which can result in arbitrary c execution. **Platforms**: win **CVEs**: CVE-2015-2509 **Refs**: source
MS13-096 Microsoft Tagged Image File Format (TIFF) Integer Overflow exploit/windows/fileformat/mswin_tiff_overflow	2013-11-05	average	This module exploits a vulnerability found i Microsoft's Tagged Image File Format. It w originally discovered in the wild, targeting Windows XP and Windows Server 2003 us running Microsoft ... **Platforms**: win **CVEs**: CVE-2013-3906 **Refs**: source, ref1, ref2
Microsoft Works 7 WkImgSrv.dll WKsPictureInterface() ActiveX Code Execution exploit/windows/fileformat/msworks_wkspictureinterface	2008-11-28	low	The Microsoft Works ActiveX control (WkImgSrv.dll) could allow a remote attack execute arbitrary code on a system. By pas a negative integer to the WksPictureInterfa method, an attacker ... **Platforms**: win **CVEs**: CVE-2008-1898 **Refs**: source

Metasploit Module	Date	Rank	Details
Microsoft Visual Basic VBP Buffer Overflow exploit/windows/fileformat/ms_visual_basic_vbp	2007-09-04	good	This module exploits a stack buffer overflo Microsoft Visual Basic 6.0. When a special crafted vbp file containing a long reference an attacker may be able to execute arbitrar code. **Platforms**: win **CVEs**: CVE-2007-4776 **Refs**: source
Steinberg MyMP3Player 3.0 Buffer Overflow exploit/windows/fileformat/mymp3player_m3u	2010-03-18	good	This module exploits a stack buffer overflo Steinberg MyMP3Player == 3.0. When the application is used to open a specially craf m3u file, a buffer overflow occurs allowing arbitrary code ... **Platforms**: win **Refs**: source
NetOp Remote Control Client 9.5 Buffer Overflow exploit/windows/fileformat/netop	2011-04-28	normal	This module exploits a stack-based buffer overflow in NetOp Remote Control 9.5. Wh opening a .dws file containing a specially c string longer then 520 characters will allow attacker to ... **Platforms**: win **Refs**: source
Nuance PDF Reader v6.0 Launch Stack Buffer Overflow exploit/windows/fileformat/nuance_pdf_launch_overflow	2010-10-08	great	This module exploits a stack buffer overflo Nuance PDF Reader v6.0. The vulnerabilit triggered when opening a malformed PDF that contains an overly long string in a /Lau field. This ... **Platforms**: win **Refs**: source, ref1
Microsoft Office DDE Payload Delivery exploit/windows/fileformat/office_dde_delivery	2017-10-09	manual	This module generates an DDE command place within a word document, that when executed, will retrieve a HTA payload via H from an web server. **Platforms**: win **Refs**: source, ref1, ref2
Microsoft Excel .SLK Payload Delivery exploit/windows/fileformat/office_excel_slk	2018-10-07	manual	This module generates a download and ex Powershell command to be placed in an .S Excel spreadsheet. When executed, it will retrieve a payload via HTTP from a web se When the file is ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
Microsoft Office CVE-2017-11882 exploit/windows/fileformat/office_ms17_11882	2017-11-15	manual	Module exploits a flaw in how the Equation Editor that allows an attacker to execute arbitrary code in RTF files without interacti The vulnerability is caused by the Equatior Editor, to which ... **Platforms**: win **CVEs**: CVE-2017-11882 **Refs**: source, ref1, ref2
Office OLE Multiple DLL Side Loading Vulnerabilities exploit/windows/fileformat/office_ole_multiple_dll_hijack	2015-12-08	normal	Multiple DLL side loading vulnerabilities we found in various COM components. These issues can be exploited by loading various these components as an embedded OLE d When instantiating a ... **Platforms**: win **CVEs**: CVE-2015-6128, CVE-2015-6132, (2015-6133, CVE-2016-0041, CVE-2016-0 CVE-2016-3235 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7, ref8, ref9, ref10, ref11
Microsoft Office Word Malicious Hta Execution exploit/windows/fileformat/office_word_hta	2017-04-14	excellent	This module creates a malicious RTF file th when opened in vulnerable versions of Mic Word will lead to code execution. The flaw exists in how a olelink object can make a h request, and ... **Platforms**: win **CVEs**: CVE-2017-0199 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7, ref8, ref9, ref10, ref11, ref12, ref13

Metasploit Module	Date	Rank	Details
OpenOffice OLE Importer DocumentSummaryInformation Stream Handling Overflow exploit/windows/fileformat/openoffice_ole	2008-04-17	normal	This module exploits a vulnerability in OpenOffice 2.3.1 and 2.3.0 on Microsoft Windows XP SP3. By supplying a OLE file a malformed DocumentSummaryInformatic stream, an attacker can gain ... **Platforms**: win **CVEs**: CVE-2008-0320 **Refs**: source, ref1
Orbital Viewer ORB File Parsing Buffer Overflow exploit/windows/fileformat/orbital_viewer_orb	2010-02-27	great	This module exploits a stack-based buffer overflow in David Manthey's Orbital Viewer When processing .ORB files, data is read f file into a fixed-size stack buffer using the f function. ... **Platforms**: win **CVEs**: CVE-2010-0688 **Refs**: source, ref1
Orbit Downloader URL Unicode Conversion Overflow exploit/windows/fileformat/orbit_download_failed_bof	2008-04-03	normal	This module exploits a stack-based buffer overflow in Orbit Downloader. The vulnerat is due to Orbit converting a URL ascii strin unicode in an insecure way with MultiByteToWideChar. The ... **Platforms**: win **CVEs**: CVE-2008-1602 **Refs**: source, ref1
VMWare OVF Tools Format String Vulnerability exploit/windows/fileformat/ovf_format_string	2012-11-08	normal	This module exploits a format string vulner in VMWare OVF Tools 2.1 for Windows. Th vulnerability occurs when printing error messages while parsing a a malformed OV file. The module has been ... **Platforms**: win **CVEs**: CVE-2012-3569 **Refs**: source, ref1
ProShow Gold v4.0.2549 (PSH File) Stack Buffer Overflow exploit/windows/fileformat/proshow_cellimage_bof	2009-08-20	great	This module exploits a stack-based buffer overflow in ProShow Gold v4.0.2549. An attacker must send the file to victim and th victim must open the file. **Platforms**: win **CVEs**: CVE-2009-3214 **Refs**: source
Photodex ProShow Producer 5.0.3256 load File Handling Buffer Overflow exploit/windows/fileformat/proshow_load_bof	2012-06-06	normal	This module exploits a stack-based buffer overflow in Photodex ProShow Producer v5.0.3256 in the handling of the plugins loa file. An attacker must send the crafted "loa to victim, who ... **Platforms**: win **Refs**: source, ref1
Publish-It PUI Buffer Overflow (SEH) exploit/windows/fileformat/publishit_pui	2014-02-05	normal	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 ... **Platforms**: win **CVEs**: CVE-2014-0980 **Refs**: source
RealNetworks RealPlayer Version Attribute Buffer Overflow exploit/windows/fileformat/realplayer_ver_attribute_bof	2013-12-20	normal	This module exploits a stack-based buffer overflow vulnerability in version 16.0.3.51 a 16.0.2.32 of RealNetworks RealPlayer, cau by improper bounds checking of the versio encoding ... **Platforms**: win **CVEs**: CVE-2013-7260 **Refs**: source, ref1
Real Networks Netzip Classic 7.5.1 86 File Parsing Buffer Overflow Vulnerability exploit/windows/fileformat/real_networks_netzip_bof	2011-01-30	good	This module exploits a stack-based buffer overflow vulnerability in version 7.5.1 86 of Networks Netzip Classic. In order for the command to be executed, an attacker mus convince someone to ... **Platforms**: win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
SafeNet SoftRemote GROUPNAME Buffer Overflow exploit/windows/fileformat/safenet_softremote_groupname	2009-10-30	good	This module exploits a stack buffer overflo SafeNet SoftRemote Security Policy Editor 10.8.5. When an attacker creates a specia formatted security policy with an overly lon GROUPNAME ... **Platforms**: win **CVEs**: CVE-2009-3861 **Refs**: source, ref1
SasCam Webcam Server v.2.6.5 Get() Method Buffer Overflow exploit/windows/fileformat/sascam_get	2008-12-29	low	The SasCam Webcam Server ActiveX con vulnerable to a buffer overflow. By passing overly long argument via the Get method, a remote attacker could overflow a buffer and execute arbitrary ... **Platforms**: win **CVEs**: CVE-2008-6898 **Refs**: source
ScadaTEC ScadaPhone Stack Buffer Overflow exploit/windows/fileformat/scadaphone_zip	2011-09-12	good	This module exploits a stack-based buffer overflow vulnerability in version 5.3.11.123 scadaTEC's ScadaPhone. In order for the command to be executed, an attacker mus convince someone to load a ... **Platforms**: win **CVEs**: CVE-2011-4535 **Refs**: source, ref1
Shadow Stream Recorder 3.0.1.7 Buffer Overflow exploit/windows/fileformat/shadow_stream_recorder_bof	2010-03-29	normal	This module exploits a buffer overflow in Shadow Stream Recorder 3.0.1.7. Using th application to open a specially crafted asx buffer overflow may occur to allow arbitrary code execution ... **Platforms**: win **CVEs**: CVE-2009-1641 **Refs**: source
PDF Shaper Buffer Overflow exploit/windows/fileformat/shaper_pdf_bof	2015-10-03	normal	PDF Shaper is prone to a security vulnerab when processing PDF files. The vulnerabili appears when we use Convert PDF to Ima and use a specially crafted PDF file. This module has been tested ... **Platforms**: win **Refs**: source
S.O.M.P.L 1.0 Player Buffer Overflow exploit/windows/fileformat/somplplayer_m3u	2010-01-22	great	This module exploits a buffer overflow in S Open Music Player v1.0. When the applica is used to import a specially crafted m3u fil buffer overflow occurs allowing arbitrary co **Platforms**: win **Refs**: source
Subtitle Processor 7.7.1 .M3U SEH Unicode Buffer Overflow exploit/windows/fileformat/subtitle_processor_m3u_bof	2011-04-26	normal	This module exploits a vulnerability found i Subtitle Processor 7. By supplying a long s of data as a .m3u file, Subtitle Processor fi converts this input in Unicode, which expar the ... **Platforms**: win **Refs**: source, ref1
Sync Breeze Enterprise 9.5.16 - Import Command Buffer Overflow exploit/windows/fileformat/syncbreeze_xml	2017-03-29	normal	This module exploits a buffer overflow in S Breeze Enterprise 9.5.16 by using the impo command option to import a specially craft xml file. **Platforms**: win **CVEs**: CVE-2017-7310 **Refs**: source
TFM MMPlayer (m3u/ppl File) Buffer Overflow exploit/windows/fileformat/tfm_mmplayer_m3u_ppl_bof	2012-03-23	good	This module exploits a buffer overflow in MMPlayer 2.2 The vulnerability is triggered when opening a malformed M3U/PPL file t contains an overly long string, which result overwriting a SEH ... **Platforms**: win **CVEs**: CVE-2009-2566 **Refs**: source

Metasploit Module	Date	Rank	Details
Total Video Player 1.3.1 (Settings.ini) - SEH Buffer Overflow exploit/windows/fileformat/total_video_player_ini_bof	2013-11-24	normal	This module exploits a buffer overflow in To Video Player 1.3.1. The vulnerability occurs opening malformed Settings.ini file e.g. "C:Program FilesTotal Video Player". This module has been tested ... **Platforms**: win **Refs**: source
TugZip 3.5 Zip File Parsing Buffer Overflow Vulnerability exploit/windows/fileformat/tugzip	2008-10-28	good	This module exploits a stack-based buffer overflow vulnerability in the latest version 3 TugZip archiving utility. In order to trigger th vulnerability, an attacker must convince someone to ... **Platforms**: win **CVEs**: CVE-2008-4779 **Refs**: source
UltraISO CCD File Parsing Buffer Overflow exploit/windows/fileformat/ultraiso_ccd	2009-04-03	great	This module exploits a stack-based buffer overflow in EZB Systems, Inc's UltraISO. W processing .CCD files, data is read from file a fixed-size stack buffer. Since no bounds checking is done, ... **Platforms**: win **CVEs**: CVE-2009-1260 **Refs**: source
UltraISO CUE File Parsing Buffer Overflow exploit/windows/fileformat/ultraiso_cue	2007-05-24	great	This module exploits a stack-based buffer overflow in EZB Systems, Inc's UltraISO. W processing .CUE files, data is read from file a fixed-size stack buffer. Since no bounds checking is done, ... **Platforms**: win **CVEs**: CVE-2007-2888 **Refs**: source
URSoft W32Dasm Disassembler Function Buffer Overflow exploit/windows/fileformat/ursoft_w32dasm	2005-01-24	good	This module exploits a buffer overflow in W32Dasm <= v8.93. By creating a malicious and convincing a user to disassemble the f with a vulnerable version of W32Dasm, the Imports/Exports ... **Platforms**: win **CVEs**: CVE-2005-0308 **Refs**: source, ref1
VariCAD 2010-2.05 EN (DWB File) Stack Buffer Overflow exploit/windows/fileformat/varicad_dwb	2010-03-17	great	This module exploits a stack-based buffer overflow in VariCAD 2010-2.05 EN. An atta must send the file to victim and the victim r open the file. **Platforms**: win **Refs**: source
VideoCharge Studio Buffer Overflow (SEH) exploit/windows/fileformat/videocharge_studio	2013-10-27	normal	This module exploits a stack based buffer overflow in VideoCharge Studio 2.12.3.685 when processing a specially crafted .VSC f This vulnerability could be exploited by a re attacker to ... **Platforms**: win **Refs**: source
VeryTools Video Spirit Pro exploit/windows/fileformat/videospirit_visprj	2011-04-11	good	This module exploits a stack buffer overflo Video Spirit <= 1.70. When opening a mali project file (.visprj), a stack buffer overflow occurs, resulting in arbitrary code executio This ... **Platforms**: win **CVEs**: CVE-2011-0499, CVE-2011-0500 **Refs**: source, ref1
Microsoft Office Visio VISIODWG.DLL DXF File Handling Vulnerability exploit/windows/fileformat/visio_dxf_bof	2010-05-04	good	This module exploits a stack based overflo vulnerability in the handling of the DXF files Microsoft Visio 2002. Revisions prior to the release of the MS bulletin MS10-028 are vulnerable. The ... **Platforms**: win **CVEs**: CVE-2010-1681 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
VisiWave VWR File Parsing Vulnerability exploit/windows/fileformat/visiwave_vwr_type	2011-05-20	great	This module exploits a vulnerability found i VisiWave's Site Survey Report application. When processing .VWR files, VisiWaveReport.exe attempts to match a v pointer based on the 'Type' property ... **Platforms**: win **CVEs**: CVE-2011-2386 **Refs**: source, ref1, ref2
VLC Media Player MKV Use After Free exploit/windows/fileformat/vlc_mkv	2018-05-24	great	This module exploits a use after free vulnerability in VideoLAN VLC =< 2.2.8. Th vulnerability exists in the parsing of MKV fi and affects both 32 bits and 64 bits. In orde exploit this, this ... **Platforms**: win **CVEs**: CVE-2018-11529 **Refs**: source, ref1
VideoLAN VLC ModPlug ReadS3M Stack Buffer Overflow exploit/windows/fileformat/vlc_modplug_s3m	2011-04-07	average	This module exploits an input validation err libmod_plugin as included with VideoLAN V 1.1.8. All versions prior to version 1.1.9 are affected. By creating a malicious S3M file, remote ... **Platforms**: win **CVEs**: CVE-2011-1574 **Refs**: source, ref1, ref2
VLC Media Player RealText Subtitle Overflow exploit/windows/fileformat/vlc_realtext	2008-11-05	good	This module exploits a stack buffer overflo vulnerability in VideoLAN VLC < 0.9.6. The vulnerability exists in the parsing of RealTe subtitle files. In order to exploit this, this mo will ... **Platforms**: win **CVEs**: CVE-2008-5036 **Refs**: source, ref1, ref2
VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow exploit/windows/fileformat/vlc_smb_uri	2009-06-24	great	This module exploits a stack-based buffer overflow in the Win32AddConnection funct the VideoLAN VLC media player. Versions through 1.0.1 are reportedly affected. This vulnerability is ... **Platforms**: win **CVEs**: CVE-2009-2484 **Refs**: source, ref1
VideoLAN VLC MKV Memory Corruption exploit/windows/fileformat/vlc_webm	2011-01-31	good	This module exploits an input validation err VideoLAN VLC < 1.1.7. By creating a malic MKV or WebM file, a remote attacker coulc execute arbitrary code. NOTE: As of July 1 2010, VLC now ... **Platforms**: win **CVEs**: CVE-2011-0531 **Refs**: source, ref1, ref2
VUPlayer CUE Buffer Overflow exploit/windows/fileformat/vuplayer_cue	2009-08-18	good	This module exploits a stack based overflo VUPlayer <= 2.49. When the application is to open a specially crafted cue file, a buffe overwritten allowing for the execution of arbitrary ... **Platforms**: win **Refs**: source
VUPlayer M3U Buffer Overflow exploit/windows/fileformat/vuplayer_m3u	2009-08-18	good	This module exploits a stack over flow in VUPlayer <= 2.49. When the application is to open a specially crafted m3u file, an buf overwritten allowing for the execution of arbitrary code. **Platforms**: win **CVEs**: CVE-2006-6251 **Refs**: source
Watermark Master Buffer Overflow (SEH) exploit/windows/fileformat/watermark_master	2013-11-01	normal	This module exploits a stack based buffer overflow in Watermark Master 2.2.23 when processing a specially crafted .WCF file. TI vulnerability could be exploited by a remote attacker to execute ... **Platforms**: win **CVEs**: CVE-2013-6935 **Refs**: source

Metasploit Module	Date	Rank	Details
Winamp MAKI Buffer Overflow exploit/windows/fileformat/winamp_maki_bof	2009-05-20	normal	This module exploits a stack based buffer overflow in Winamp 5.55. The flaw exists in gen_ff.dll and occurs while parsing a speci crafted MAKI file, where memmove is usec an insecure way ... **Platforms**: win **CVEs**: CVE-2009-1831 **Refs**: source, ref1
RARLAB WinRAR ACE Format Input Validation Remote Code Execution exploit/windows/fileformat/winrar_ace	2019-02-05	excellent	In WinRAR versions prior to and including there is path traversal vulnerability when cr the filename field of the ACE format (in UNACEV2.dll). When the filename field is manipulated with ... **Platforms**: win **CVEs**: CVE-2018-20250 **Refs**: source, ref1, ref2, ref3
WinRAR Filename Spoofing exploit/windows/fileformat/winrar_name_spoofing	2009-09-28	excellent	This module abuses a filename spoofing vulnerability in WinRAR. The vulnerability e when opening ZIP files. The file names sho in WinRAR when opening a ZIP file come f the central ... **Platforms**: win **Refs**: source, ref1, ref2
Wireshark wiretap/mpeg.c Stack Buffer Overflow exploit/windows/fileformat/wireshark_mpeg_overflow	2014-03-20	good	This module triggers a stack buffer overflo Wireshark <= 1.8.12/1.10.5 by generating a malicious file. **Platforms**: win **CVEs**: CVE-2014-2299 **Refs**: source, ref1, ref2
Wireshark packet-dect.c Stack Buffer Overflow (local) exploit/windows/fileformat/wireshark_packet_dect	2011-04-18	good	This module exploits a stack buffer overflo Wireshark <= 1.4.4 When opening a malici .pcap file in Wireshark, a stack buffer occu resulting in arbitrary code execution. Note: exploit the ... **Platforms**: win **CVEs**: CVE-2011-1591 **Refs**: source, ref1, ref2
WM Downloader 3.1.2.2 Buffer Overflow exploit/windows/fileformat/wm_downloader_m3u	2010-07-28	normal	This module exploits a buffer overflow in W Downloader v3.1.2.2. When the applicatior used to import a specially crafted m3u file, buffer overflow occurs allowing arbitrary co execution. **Platforms**: win **Refs**: source
Xenorate 2.50 (.xpl) Universal Local Buffer Overflow (SEH) exploit/windows/fileformat/xenorate_xpl_bof	2009-08-19	great	This module exploits a stack buffer overflo Xenorate 2.50 by creating a specially crafte file. **Platforms**: win **Refs**: source
Xion Audio Player 1.0.126 Unicode Stack Buffer Overflow exploit/windows/fileformat/xion_m3u_sehbof	2010-11-23	great	This module exploits a stack buffer overflo Xion Audio Player prior to version 1.0.126. vulnerability is triggered when opening a malformed M3U file that contains an overly string. This ... **Platforms**: win **Refs**: source
xRadio 0.95b Buffer Overflow exploit/windows/fileformat/xradio_xrl_sehbof	2011-02-08	normal	This module exploits a buffer overflow in xF 0.95b. Using the application to import a specially crafted xrl file, a buffer overflow o allowing arbitrary code execution. **Platforms**: win **CVEs**: CVE-2008-2789 **Refs**: source
Zahir Enterprise Plus 6 Stack Buffer Overflow exploit/windows/fileformat/zahir_enterprise_plus_csv	2018-09-28	normal	This module exploits a stack buffer overflo Zahir Enterprise Plus version 6 build 10b a below. The vulnerability is triggered when opening a CSV file containing CR/LF and c long string ... **Platforms**: win **CVEs**: CVE-2018-17408 **Refs**: source

Metasploit Module	Date	Rank	Details
Zinf Audio Player 2.2.1 (PLS File) Stack Buffer Overflow exploit/windows/fileformat/zinfaudioplayer221_pls	2004-09-24	good	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 ma possible to ... **Platforms**: win **CVEs**: CVE-2004-0964 **Refs**: source
ISS PAM.dll ICQ Parser Buffer Overflow exploit/windows/firewall/blackice_pam_icq	2004-03-18	great	This module exploits a stack buffer overflow the ISS products that use the iss-pam1.dll parser (Blackice/RealSecure). Successful exploitation will result in arbitrary code execution as ... **Platforms**: win **CVEs**: CVE-2004-0362 **Refs**: source, ref1
Kerio Firewall 2.1.4 Authentication Packet Overflow exploit/windows/firewall/kerio_auth	2003-04-28	average	This module exploits a stack buffer overflow Kerio Personal Firewall administration authentication process. This module has o been tested against Kerio Personal Firewa (2.1.4). **Platforms**: win **CVEs**: CVE-2003-0220 **Refs**: source
FileWrangler 5.30 Stack Buffer Overflow exploit/windows/ftp/filewrangler_list_reply	2010-10-12	good	This module exploits a buffer overflow in th FileWrangler client that is triggered when tl client connects to a FTP server and lists th directory contents, containing an overly lon directory name. **Platforms**: win **Refs**: source, ref1
LeapWare LeapFTP v2.7.3.600 PASV Reply Client Overflow exploit/windows/ftp/leapftp_pasv_reply	2003-06-09	normal	This module exploits a buffer overflow in th LeapWare LeapFTP v2.7.3.600 client that triggered through an excessively long PAS reply command. This module was ported fr the original exploit by ... **Platforms**: win **CVEs**: CVE-2003-0558 **Refs**: source
32bit FTP Client Stack Buffer Overflow exploit/windows/ftp/32bitftp_list_reply	2010-10-12	good	This module exploits a stack buffer overflow 32bit ftp client, triggered when trying to download a file that has an overly long filer **Platforms**: win **Refs**: source, ref1
3Com 3CDaemon 2.0 FTP Username Overflow exploit/windows/ftp/3cdaemon_ftp_user	2005-01-04	average	This module exploits a vulnerability in the 3 3CDaemon FTP service. This package is b distributed from the 3Com web site and is recommended in numerous support docum This module uses the ... **Platforms**: win **CVEs**: CVE-2005-0277 **Refs**: source
AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST) exploit/windows/ftp/aasync_list_reply	2010-10-12	good	This module exploits a stack buffer overflow AASync v2.2.1.0, triggered when processir response on a LIST command. During the overflow, a structured exception handler re gets overwritten. **Platforms**: win **Refs**: source, ref1
Ability Server 2.34 STOR Command Stack Buffer Overflow exploit/windows/ftp/ability_server_stor	2004-10-22	normal	This module exploits a stack-based buffer overflow in Ability Server 2.34. Ability Serv fails to check input size when parsing 'STC and 'APPE' commands, which leads to a st based buffer ... **Platforms**: win **CVEs**: CVE-2004-1626 **Refs**: source

Metasploit Module	Date	Rank	Details
AbsoluteFTP 1.9.6 - 2.2.10 LIST Command Remote Buffer Overflow exploit/windows/ftp/absolute_ftp_list_bof	2011-11-09	normal	This module exploits VanDyke Software AbsoluteFTP by overflowing a filename bu related to the LIST command. **Platforms**: win **CVEs**: CVE-2011-5164 **Refs**: source
Ayukov NFTP FTP Client Buffer Overflow exploit/windows/ftp/ayukov_nftp	2017-10-21	normal	This module exploits a stack-based buffer overflow vulnerability against Ayukov NFTF FTP Client 2.0 and earlier. By responding v long string of data for the SYST request, it possible to ... **Platforms**: win **CVEs**: CVE-2017-15222 **Refs**: source
BisonWare BisonFTP Server Buffer Overflow exploit/windows/ftp/bison_ftp_bof	2011-08-07	normal	BisonWare BisonFTP Server 3.5 is prone t overflow condition. This module exploits a overflow vulnerability in the said applicatio **Platforms**: win **CVEs**: CVE-1999-1510 **Refs**: source, ref1
Cesar FTP 0.99g MKD Command Buffer Overflow exploit/windows/ftp/cesarftp_mkd	2006-06-12	average	This module exploits a stack buffer overflo the MKD verb in CesarFTP 0.99g. You mu have valid credentials to trigger this vulnera Also, you only get one chance, so choose target ... **Platforms**: win **CVEs**: CVE-2006-2961 **Refs**: source, ref1
ComSndFTP v1.3.7 Beta USER Format String (Write4) Vulnerability exploit/windows/ftp/comsnd_ftpd_fmtstr	2012-06-08	good	This module exploits the ComSndFTP FTP Server version 1.3.7 beta by sending a spe crafted format string specifier as a usernan The crafted username is sent to the server overwrite the ... **Platforms**: win **Refs**: source
BolinTech Dream FTP Server 1.02 Format String exploit/windows/ftp/dreamftp_format	2004-03-03	good	This module exploits a format string overflo the BolinTech Dream FTP Server version 1 Based on the exploit by SkyLined. **Platforms**: win **CVEs**: CVE-2004-2074 **Refs**: source
Easy File Sharing FTP Server 2.0 PASS Overflow exploit/windows/ftp/easyfilesharing_pass	2006-07-31	average	This module exploits a stack buffer overflo the Easy File Sharing 2.0 service. By send an overly long password, an attacker can execute arbitrary code. **Platforms**: win **CVEs**: CVE-2006-3952 **Refs**: source
EasyFTP Server CWD Command Stack Buffer Overflow exploit/windows/ftp/easyftp_cwd_fixret	2010-02-16	great	This module exploits a stack-based buffer overflow in EasyFTP Server 1.7.0.11 and e EasyFTP fails to check input size when pa 'CWD' commands, which leads to a stack b buffer overflow. ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
EasyFTP Server LIST Command Stack Buffer Overflow exploit/windows/ftp/easyftp_list_fixret	2010-07-05	great	This module exploits a stack-based buffer overflow in EasyFTP Server 1.7.0.11. cred goes to Karn Ganeshan. NOTE: Although, is likely to exploit the same vulnerability as ... **Platforms**: win **Refs**: source
EasyFTP Server MKD Command Stack Buffer Overflow exploit/windows/ftp/easyftp_mkd_fixret	2010-04-04	great	This module exploits a stack-based buffer overflow in EasyFTP Server 1.7.0.11 and e EasyFTP fails to check input size when pa 'MKD' commands, which leads to a stack b buffer overflow. ... **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
FileCopa FTP Server Pre 18 Jul Version exploit/windows/ftp/filecopa_list_overflow	2006-07-19	average	This module exploits the buffer overflow fo the LIST command in fileCOPA FTP serve 18 Jul 2006 version discovered by www.appsec.ch. **Platforms**: win **CVEs**: CVE-2006-3726 **Refs**: source
Free Float FTP Server USER Command Buffer Overflow exploit/windows/ftp/freefloatftp_user	2012-06-12	normal	Freefloat FTP Server is prone to an overflo condition. It fails to properly sanitize user-supplied input resulting in a stack-based bu overflow. With a specially crafted 'USER' command, a remote ... **Platforms**: win **Refs**: source
FreeFloat FTP Server Arbitrary File Upload exploit/windows/ftp/freefloatftp_wbem	2012-12-07	excellent	This module abuses multiple issues in FreeFloat: 1. No credential is actually neec login, 2. User's default path is in C:, and th cannot be changed, 3. User can write to anywhere on the ... **Platforms**: win **Refs**: source
freeFTPd PASS Command Buffer Overflow exploit/windows/ftp/freeftpd_pass	2013-08-20	normal	freeFTPd 1.0.10 and below contains an overflow condition that is triggered as user-supplied input is not properly validated whe handling a specially crafted PASS commar This may allow a remote ... **Platforms**: win **Refs**: source
freeFTPd 1.0 Username Overflow exploit/windows/ftp/freeftpd_user	2005-11-16	average	This module exploits a stack buffer overflo the freeFTPd multi-protocol file transfer ser This flaw can only be exploited when loggi has been enabled (non-default). **Platforms**: win **CVEs**: CVE-2005-3683 **Refs**: source
FTPGetter Standard v3.55.0.05 Stack Buffer Overflow (PWD) exploit/windows/ftp/ftpgetter_pwd_reply	2010-10-12	good	This module exploits a buffer overflow in FTPGetter Standard v3.55.0.05 ftp client. V processing the response on a PWD comm a stack based buffer overflow occurs. This to arbitrary code ... **Platforms**: win **Refs**: source, ref1
FTPPad 1.2.0 Stack Buffer Overflow exploit/windows/ftp/ftppad_list_reply	2010-10-12	good	This module exploits a stack buffer overflo FTPPad 1.2.0 ftp client. The overflow is triggered when the client connects to a FT server which sends an overly long directory filename in response ... **Platforms**: win **Refs**: source, ref1
FTPShell 5.1 Stack Buffer Overflow exploit/windows/ftp/ftpshell51_pwd_reply	2010-10-12	good	This module exploits a stack buffer overflo FTPShell 5.1. The overflow gets triggered the ftp client tries to process an overly long response to a PWD command. This will overwrite the saved ... **Platforms**: win **Refs**: source, ref1
FTPShell client 6.70 (Enterprise edition) Stack Buffer Overflow exploit/windows/ftp/ftpshell_cli_bof	2017-03-04	normal	This module exploits a buffer overflow in th FTPShell client 6.70 (Enterprise edition) allowing remote code execution. **Platforms**: win **CVEs**: CVE-2018-7573 **Refs**: source
FTP Synchronizer Professional 4.0.73.274 Stack Buffer Overflow exploit/windows/ftp/ftpsynch_list_reply	2010-10-12	good	This module exploits a stack buffer overflo vulnerability in FTP Synchronizer Pro versi 4.0.73.274 The overflow gets triggered by sending an overly long filename to the clier response to a ... **Platforms**: win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Gekko Manager FTP Client Stack Buffer Overflow exploit/windows/ftp/gekkomgr_list_reply	2010-10-12	good	This module exploits a buffer overflow in G Manager ftp client, triggered when process the response received after sending a LIST request. If this response contains a long filename, a buffer ... **Platforms**: win **Refs**: source, ref1
GlobalSCAPE Secure FTP Server Input Overflow exploit/windows/ftp/globalscapeftp_input	2005-05-01	great	This module exploits a buffer overflow in th GlobalSCAPE Secure FTP Server. All vers prior to 3.0.3 are affected by this flaw. A va user account (or anonymous access) is required for this ... **Platforms**: win **CVEs**: CVE-2005-1415 **Refs**: source, ref1
GoldenFTP PASS Stack Buffer Overflow exploit/windows/ftp/goldenftp_pass_bof	2011-01-23	average	This module exploits a vulnerability in the Golden FTP service, using the PASS comr to cause a buffer overflow. Please note tha order trigger the vulnerable code, the victin machine must have ... **Platforms**: win **CVEs**: CVE-2006-6576 **Refs**: source
HTTPDX tolog() Function Format String Vulnerability exploit/windows/ftp/httpdx_tolog_format	2009-11-17	great	This module exploits a format string vulner in HTTPDX FTP server. By sending a spec crafted FTP command containing format specifiers, an attacker can corrupt memory execute arbitrary ... **Platforms**: win **CVEs**: CVE-2009-4769 **Refs**: source
Konica Minolta FTP Utility 1.00 Post Auth CWD Command SEH Overflow exploit/windows/ftp/kmftp_utility_cwd	2015-08-23	normal	This module exploits an SEH overflow in K Minolta FTP Server 1.00. Konica Minolta F fails to check input size when parsing 'CWI commands, which leads to an SEH overflo Konica FTP allows ... **Platforms**: win **CVEs**: CVE-2015-7768 **Refs**: source
LabF nfsAxe 3.7 FTP Client Stack Buffer Overflow exploit/windows/ftp/labf_nfsaxe	2017-05-15	normal	This module exploits a buffer overflow in th LabF nfsAxe 3.7 FTP Client allowing remot code execution. **Platforms**: win **CVEs**: CVE-2017-18047 **Refs**: source
LeapFTP 3.0.1 Stack Buffer Overflow exploit/windows/ftp/leapftp_list_reply	2010-10-12	good	This module exploits a buffer overflow in th LeapFTP 3.0.1 client. This issue is triggere when a file with a long name is downloaded/opened. **Platforms**: win **Refs**: source, ref1
MS09-053 Microsoft IIS FTP Server NLST Response Overflow exploit/windows/ftp/ms09_053_ftpd_nlst	2009-08-31	great	This module exploits a stack buffer overflo in the Microsoft IIS FTP service. The flaw is triggered when a special NLST argument is passed while the session has changed into long directory ... **Platforms**: win **CVEs**: CVE-2009-3023 **Refs**: source
NetTerm NetFTPD USER Buffer Overflow exploit/windows/ftp/netterm_netftpd_user	2005-04-26	great	This module exploits a vulnerability in the NetTerm NetFTPD application. This packa part of the NetTerm package. This module the USER command to trigger the overflow **Platforms**: win **CVEs**: CVE-2005-1323 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Odin Secure FTP 4.1 Stack Buffer Overflow (LIST) exploit/windows/ftp/odin_list_reply	2010-10-12	good	This module exploits a stack buffer overflo Odin Secure FTP 4.1, triggered when processing the response on a LIST comma During the overflow, a structured exception handler record gets ... **Platforms**: win **Refs**: source, ref1
Open-FTPD 1.2 Arbitrary File Upload exploit/windows/ftp/open_ftpd_wbem	2012-06-18	excellent	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 ... **Platforms**: win **CVEs**: CVE-2010-2620 **Refs**: source
Oracle 9i XDB FTP PASS Overflow (win32) exploit/windows/ftp/oracle9i_xdb_ftp_pass	2003-08-18	great	By passing an overly long string to the PAS command, a stack based buffer overflow o David Litchfield, has illustrated multiple vulnerabilities in the Oracle 9i XML Databa (XDB), during a ... **Platforms**: win **CVEs**: CVE-2003-0727 **Refs**: source, ref1
Oracle 9i XDB FTP UNLOCK Overflow (win32) exploit/windows/ftp/oracle9i_xdb_ftp_unlock	2003-08-18	great	By passing an overly long token to the UNL command, a stack based buffer overflow o David Litchfield, has illustrated multiple vulnerabilities in the Oracle 9i XML Databa (XDB), during a ... **Platforms**: win **CVEs**: CVE-2003-0727 **Refs**: source, ref1
PCMAN FTP Server Buffer Overflow - PUT Command exploit/windows/ftp/pcman_put	2015-08-07	normal	This module exploits a buffer overflow vulnerability found in the PUT command of PCMAN FTP v2.0.7 Server. This requires authentication but by default anonymous credentials are enabled. **Platforms**: win **CVEs**: CVE-2013-4730 **Refs**: source
PCMAN FTP Server Post-Authentication STOR Command Stack Buffer Overflow exploit/windows/ftp/pcman_stor	2013-06-27	normal	This module exploits a buffer overflow vulnerability found in the STOR command PCMAN FTP v2.07 Server when the "/./" parameters are also sent to the server. Ple note authentication is ... **Platforms**: win **CVEs**: CVE-2013-4730 **Refs**: source
ProFTP 2.9 Banner Remote Buffer Overflow exploit/windows/ftp/proftp_banner	2009-08-25	normal	This module exploits a buffer overflow in th ProFTP 2.9 client that is triggered through excessively long welcome message. **Platforms**: win **CVEs**: CVE-2009-3976 **Refs**: source, ref1
QuickShare File Server 1.2.1 Directory Traversal Vulnerability exploit/windows/ftp/quickshare_traversal_write	2011-02-03	excellent	This module exploits a vulnerability found i QuickShare File Server's FTP service. By supplying "./" in the file path, it is possible t trigger a directory traversal flaw, allowing th attacker to ... **Platforms**: win **Refs**: source, ref1, ref2
Ricoh DC DL-10 SR10 FTP USER Command Buffer Overflow exploit/windows/ftp/ricoh_dl_bof	2012-03-01	normal	This module exploits a vulnerability found i 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-b buffer overflow, which ... **Platforms**: win **CVEs**: CVE-2012-5002 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Sami FTP Server LIST Command Buffer Overflow exploit/windows/ftp/sami_ftpd_list	2013-02-27	low	This module exploits a stack based buffer overflow on Sami FTP Server 2.0.1. The vulnerability exists in the processing of LIS commands. In order to trigger the vulnerab the "Log" tab must be ... **Platforms**: win **Refs**: source
KarjaSoft Sami FTP Server v2.0.2 USER Overflow exploit/windows/ftp/sami_ftpd_user	2006-01-24	normal	This module exploits an unauthenticated st buffer overflow in KarjaSoft Sami FTP Serv version 2.0.2 by sending an overly long US string during login. The payload is triggered when the ... **Platforms**: win **CVEs**: CVE-2006-0441, CVE-2006-2212 **Refs**: source
Sasser Worm avserve FTP PORT Buffer Overflow exploit/windows/ftp/sasser_ftpd_port	2004-05-10	average	This module exploits the FTP server compo of the Sasser worm. By sending an overly PORT command the stack can be overwrit **Platforms**: win **Refs**: source
ScriptFTP LIST Remote Buffer Overflow exploit/windows/ftp/scriptftp_list	2011-10-12	good	AmmSoft's ScriptFTP client is susceptible t remote buffer overflow vulnerability that is triggered when processing a sufficiently lor filename during a FTP LIST command resu in overwriting ... **Platforms**: win **CVEs**: CVE-2011-3976 **Refs**: source
Seagull FTP v3.3 Build 409 Stack Buffer Overflow exploit/windows/ftp/seagull_list_reply	2010-10-12	good	This module exploits a buffer overflow in th Seagull FTP client that gets triggered wher ftp client processes a response to a LIST command. If the response contains an ove long file/folder ... **Platforms**: win **Refs**: source, ref1
Serv-U FTP Server Buffer Overflow exploit/windows/ftp/servu_chmod	2004-12-31	normal	This module exploits a stack buffer overflo the site chmod command in versions of Se FTP Server prior to 4.2. You must have val credentials to trigger this vulnerability. Exploitation also ... **Platforms**: win **CVEs**: CVE-2004-2111 **Refs**: source
Serv-U FTPD MDTM Overflow exploit/windows/ftp/servu_mdtm	2004-02-26	good	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 ... **Platforms**: win **CVEs**: CVE-2004-0330 **Refs**: source, ref1
SlimFTPd LIST Concatenation Overflow exploit/windows/ftp/slimftpd_list_concat	2005-07-21	great	This module exploits a stack buffer overflo the SlimFTPd server. The flaw is triggered a LIST command is received with an overly argument. This vulnerability affects all vers of ... **Platforms**: win **CVEs**: CVE-2005-2373 **Refs**: source
Trellian FTP Client 3.01 PASV Remote Buffer Overflow exploit/windows/ftp/trellian_client_pasv	2010-04-11	normal	This module exploits a buffer overflow in th Trellian 3.01 FTP client that is triggered thr an excessively long PASV message. **Platforms**: win **CVEs**: CVE-2010-1465 **Refs**: source
Turbo FTP Server 1.30.823 PORT Overflow exploit/windows/ftp/turboftp_port	2012-10-03	great	This module exploits a buffer overflow vulnerability found in the PORT command Turbo FTP Server 1.30.823 1.30.826, whic results in remote code execution under the context of SYSTEM. ... **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
Vermillion FTP Daemon PORT Command Memory Corruption exploit/windows/ftp/vermillion_ftpd_port	2009-09-23	great	This module exploits an out-of-bounds arra access in the Arcane Software Vermillion F server. By sending a specially crafted FTP PORT command, an attacker can corrupt s memory and execute ... **Platforms**: win **Refs**: source
War-FTPD 1.65 Password Overflow exploit/windows/ftp/warftpd_165_pass	1998-03-19	average	This exploits the buffer overflow found in th PASS command in War-FTPD 1.65. This particular module will only work reliably aga Windows 2000 targets. The server must be configured to allow ... **Platforms**: win **CVEs**: CVE-1999-0256 **Refs**: source
War-FTPD 1.65 Username Overflow exploit/windows/ftp/warftpd_165_user	1998-03-19	average	This module exploits a buffer overflow four the USER command of War-FTPD 1.65. **Platforms**: win **CVEs**: CVE-1999-0256 **Refs**: source
Texas Imperial Software WFTPD 3.23 SIZE Overflow exploit/windows/ftp/wftpd_size	2006-08-23	average	This module exploits a buffer overflow in th SIZE verb in Texas Imperial's Software WF 3.23. **Platforms**: win **CVEs**: CVE-2006-4318 **Refs**: source
WinaXe 7.7 FTP Client Remote Buffer Overflow exploit/windows/ftp/winaxe_server_ready	2016-11-03	good	This module exploits a buffer overflow in th WinaXe 7.7 FTP client. This issue is trigge when a client connects to the server and is expecting the Server Ready response. **Platforms**: win **Refs**: source, ref1
Wing FTP Server Authenticated Command Execution exploit/windows/ftp/wing_ftp_admin_exec	2014-06-19	excellent	This module exploits the embedded Lua interpreter in the admin web interface for versions 3.0.0 and above. When supplying specially crafted HTTP POST request an attacker can use os.execute() to ... **Platforms**: win **Refs**: source, ref1, ref2
WS-FTP Server 5.03 MKD Overflow exploit/windows/ftp/wsftp_server_503_mkd	2004-11-29	great	This module exploits the buffer overflow fo the MKD command in IPSWITCH WS_FTP Server 5.03 discovered by Reed Arvin. **Platforms**: win **CVEs**: CVE-2004-1135 **Refs**: source
Ipswitch WS_FTP Server 5.05 XMD5 Overflow exploit/windows/ftp/wsftp_server_505_xmd5	2006-09-14	average	This module exploits a buffer overflow in th XMD5 verb in IPSWITCH WS_FTP Server **Platforms**: win **CVEs**: CVE-2006-4847 **Refs**: source
Xftp FTP Client 3.0 PWD Remote Buffer Overflow exploit/windows/ftp/xftp_client_pwd	2010-04-22	normal	This module exploits a buffer overflow in th Xftp 3.0 FTP client that is triggered through excessively long PWD message. **Platforms**: win **Refs**: source
Xlink FTP Client Buffer Overflow exploit/windows/ftp/xlink_client	2009-10-03	normal	This module exploits a stack buffer overflo Xlink FTP Client 32 Version 3.01 that come bundled with Omni-NFS Enterprise 5.2. Wh an overly long FTP server response is rece by a client, ... **Platforms**: win **CVEs**: CVE-2006-5792 **Refs**: source, ref1
Xlink FTP Server Buffer Overflow exploit/windows/ftp/xlink_server	2009-10-03	good	This module exploits a stack buffer overflo Xlink FTP Server that comes bundled with Omni-NFS Enterprise 5.2. When a overly l FTP request is sent to the server, arbitrary may be executed. **Platforms**: win **CVEs**: CVE-2006-5792 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Medal of Honor Allied Assault getinfo Stack Buffer Overflow exploit/windows/games/mohaa_getinfo	2004-07-17	great	This module exploits a stack based buffer overflow in the getinfo command of Medal Honor Allied Assault. **Platforms**: win **CVEs**: CVE-2004-0735 **Refs**: source
Racer v0.5.3 Beta 5 Buffer Overflow exploit/windows/games/racer_503beta5	2008-08-10	great	This module exploits the Racer Car and Ra Simulator game versions v0.5.3 beta 5 and earlier. Both the client and server listen on port 26000. By sending an overly long buff are able to ... **Platforms**: win **CVEs**: CVE-2007-4370 **Refs**: source
Unreal Tournament 2004 "secure" Overflow (Win32) exploit/windows/games/ut2004_secure	2004-06-18	good	This is an exploit for the GameSpy secure in the Unreal Engine. This exploit only requ one UDP packet, which can be both spoofe and sent to a broadcast address. Usually, t GameSpy query ... **Platforms**: win **CVEs**: CVE-2004-0608 **Refs**: source
Adobe RoboHelp Server 8 Arbitrary File Upload and Execute exploit/windows/http/adobe_robohelper_authbypass	2009-09-23	excellent	This module exploits an authentication byp vulnerability which allows remote attackers upload and execute arbitrary code. **Platforms**: win **CVEs**: CVE-2009-3068 **Refs**: source, ref1
Advantech iView Unauthenticated Remote Code Execution exploit/windows/http/advantech_iview_unauth_rce	2021-02-09	excellent	This module exploits an unauthenticated configuration change combined with an unauthenticated file write primitive, leading arbitrary file write that allows for remote co execution as the ... **Platforms**: win **CVEs**: CVE-2021-22652 **Refs**: source, ref1, ref2
Alt-N SecurityGateway username Buffer Overflow exploit/windows/http/altn_securitygateway	2008-06-02	average	Alt-N SecurityGateway is prone to a buffer overflow condition. This is due to insufficien bounds checking on the "username" param Successful exploitation could result in code execution with ... **Platforms**: win **CVEs**: CVE-2008-4193 **Refs**: source
Alt-N WebAdmin USER Buffer Overflow exploit/windows/http/altn_webadmin	2003-06-24	average	Alt-N WebAdmin is prone to a buffer overfl condition. This is due to insufficient bounds checking on the USER parameter. Succes exploitation could result in code execution SYSTEM level ... **Platforms**: win **CVEs**: CVE-2003-0471 **Refs**: source, ref1
Amlibweb NetOpacs webquery.dll Stack Buffer Overflow exploit/windows/http/amlibweb_webquerydll_app	2010-08-03	normal	This module exploits a stack buffer overflo Amlib's Amlibweb Library Management Sy (NetOpacs). The webquery.dll API is availa through IIS requests. By specifying an ove long string to ... **Platforms**: win **Refs**: source, ref1
Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload exploit/windows/http/apache_activemq_traversal_upload	2015-08-19	excellent	This module exploits a directory traversal vulnerability (CVE-2015-1830) in Apache ActiveMQ 5.x before 5.11.2 for Windows. T module tries to upload a JSP payload to th /admin directory via the ... **Platforms**: win **CVEs**: CVE-2015-1830 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Apache Win32 Chunked Encoding exploit/windows/http/apache_chunked	2002-06-19	good	This module exploits the chunked transfer integer wrap vulnerability in Apache versio 1.2.x to 1.3.24. This particular module has tested with all versions of the official Win32 between ... **Platforms**: win **CVEs**: CVE-2002-0392 **Refs**: source
Apache mod_jk 1.2.20 Buffer Overflow exploit/windows/http/apache_modjk_overflow	2007-03-02	great	This is a stack buffer overflow exploit for m 1.2.20. Should work on any Win32 OS. **Platforms**: win **CVEs**: CVE-2007-0774 **Refs**: source
Apache Module mod_rewrite LDAP Protocol Buffer Overflow exploit/windows/http/apache_mod_rewrite_ldap	2006-07-28	great	This module exploits the mod_rewrite LDA protocol scheme handling flaw discovered Mark Dowd, which produces an off-by-one overflow. Apache versions 1.3.29-36, 2.0.4 and 2.2.1-2 are ... **Platforms**: win **CVEs**: CVE-2006-3747 **Refs**: source, ref1
Apache Tika Header Command Injection exploit/windows/http/apache_tika_jp2_jscript	2018-04-25	excellent	This module exploits a command injection vulnerability in Apache Tika 1.15 - 1.17 on Windows. A file with the image/jp2 content is used to bypass magic bytes checking. W OCR is specified in ... **Platforms**: win **CVEs**: CVE-2018-1335 **Refs**: source, ref1, ref2
Avaya IP Office Customer Call Reporter ImageUpload.ashx Remote Command Execution exploit/windows/http/avaya_ccr_imageupload_exec	2012-06-28	excellent	This module exploits an authentication byp vulnerability on Avaya IP Office Customer Reporter, which allows a remote user to up arbitrary files through the ImageUpload.ash component. It ... **Platforms**: win **CVEs**: CVE-2012-3811 **Refs**: source, ref1
BadBlue 2.5 EXT.dll Buffer Overflow exploit/windows/http/badblue_ext_overflow	2003-04-20	great	This is a stack buffer overflow exploit for BadBlue version 2.5. **Platforms**: win **CVEs**: CVE-2005-0595 **Refs**: source
BadBlue 2.72b PassThru Buffer Overflow exploit/windows/http/badblue_passthru	2007-12-10	great	This module exploits a stack buffer overflo the PassThru functionality in ext.dll in BadB 2.72b and earlier. **Platforms**: win **CVEs**: CVE-2007-6377 **Refs**: source
BEA WebLogic JSESSIONID Cookie Value Overflow exploit/windows/http/bea_weblogic_jsessionid	2009-01-13	good	This module exploits a buffer overflow in B WebLogic plugin. The vulnerable code is o accessible when clustering is configured. A request containing a long JSESSION cook value can lead to ... **Platforms**: win **CVEs**: CVE-2008-5457 **Refs**: source
BEA Weblogic Transfer-Encoding Buffer Overflow exploit/windows/http/bea_weblogic_transfer_encoding	2008-09-09	great	This module exploits a stack based buffer overflow in the BEA Weblogic Apache plug This vulnerability exists in the error reportir unknown Transfer-Encoding headers. You have to run this ... **Platforms**: win **CVEs**: CVE-2008-4008 **Refs**: source
Belkin Bulldog Plus Web Service Buffer Overflow exploit/windows/http/belkin_bulldog	2009-03-08	average	This module exploits a stack buffer overflo Belkin Bulldog Plus 4.0.2 build 1219. Wher sending a specially crafted http request, ar attacker may be able to execute arbitrary c **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
Cayin xPost wayfinder_seqid SQLi to RCE exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	This module exploits an unauthenticated S in Cayin xPost <=2.5. The wayfinder_meeting_input.jsp file's wayfinder_seqid parameter can be injectec a blind SQLi. Since this app bundles MySC and ... **Platforms**: java, win **CVEs**: CVE-2020-7356 **Refs**: source, ref1
CA Arcserve D2D GWT RPC Credential Information Disclosure exploit/windows/http/ca_arcserve_rpc_authbypass	2011-07-25	excellent	This module exploits an information disclos vulnerability in the CA Arcserve D2D r15 w server. The information disclosure can be triggered by sending a specially crafted RF request to the ... **Platforms**: win **CVEs**: CVE-2011-3011 **Refs**: source
CA iTechnology iGateway Debug Mode Buffer Overflow exploit/windows/http/ca_igateway_debug	2005-10-06	average	This module exploits a vulnerability in the Computer Associates iTechnology iGatewa component. When True is enabled in igateway.conf (non-default), it is possible tc overwrite the ... **Platforms**: win **CVEs**: CVE-2005-3190 **Refs**: source, ref1
CA Total Defense Suite reGenerateReports Stored Procedure SQL Injection exploit/windows/http/ca_totaldefense_regeneratereports	2011-04-13	excellent	This module exploits a SQL injection flaw i Total Defense Suite R12. When supplying a specially crafted soap request to '/UNCWS/Management.asmx', an attacker abuse the reGenerateReports ... **Platforms**: win **CVEs**: CVE-2011-1653 **Refs**: source
Cogent DataHub Command Injection exploit/windows/http/cogent_datahub_command	2014-04-29	manual	This module exploits an injection vulnerabi Cogent DataHub prior to 7.3.5. The vulnera exists in the GetPermissions.asp page, wh makes insecure use of the datahub_comm function ... **Platforms**: win **CVEs**: CVE-2014-3789 **Refs**: source
Cogent DataHub HTTP Server Buffer Overflow exploit/windows/http/cogent_datahub_request_headers_bof	2013-07-26	normal	This module exploits a stack based buffer overflow on Cogent DataHub 7.3.0. The vulnerability exists in the HTTP server. Wh handling HTTP headers, a strncpy() functic used in a dangerous way. ... **Platforms**: win **CVEs**: CVE-2013-0680 **Refs**: source, ref1
ColdFusion 8.0.1 Arbitrary File Upload and Execute exploit/windows/http/coldfusion_fckeditor	2009-07-03	excellent	This module exploits the Adobe ColdFusio 8.0.1 FCKeditor 'CurrentFolder' File Upload Execute vulnerability. **Platforms**: win **CVEs**: CVE-2009-2265 **Refs**: source
Cyclope Employee Surveillance Solution v6 SQL Injection exploit/windows/http/cyclope_ess_sqli	2012-08-08	excellent	This module exploits a SQL injection found Cyclope Employee Surveillance Solution. Because the login script does not properly handle the user-supplied username param a malicious user can ... **Platforms**: win **Refs**: source
ManageEngine Desktop Central Java Deserialization exploit/windows/http/desktopcentral_deserialization	2020-03-05	excellent	This module exploits a Java deserializatior vulnerability in the getChartImage() metho from the FileStorage class within ManageEngine Desktop Central versions < 10.0.474. Tested against 10.0.465 ... **Platforms**: win **CVEs**: CVE-2020-10189 **Refs**: source, ref1, ref2, ref3, ref4

Metasploit Module	Date	Rank	Details
ManageEngine Desktop Central AgentLogUpload Arbitrary File Upload exploit/windows/http/desktopcentral_file_upload	2013-11-11	excellent	This module exploits an arbitrary file uploa vulnerability in Desktop Central v7 to v8 bu 80293. A malicious user can upload a JSP into the web root without authentication, lea to ... **Platforms**: win **CVEs**: CVE-2013-7390 **Refs**: source, ref1, ref2
ManageEngine Desktop Central StatusUpdate Arbitrary File Upload exploit/windows/http/desktopcentral_statusupdate_upload	2014-08-31	excellent	This module exploits an arbitrary file uploa vulnerability in ManageEngine DesktopCer v7 to v9 build 90054 (including the MSP versions). A malicious user can upload a J file into the web root ... **Platforms**: win **CVEs**: CVE-2014-5005 **Refs**: source, ref1
DiskBoss Enterprise GET Buffer Overflow exploit/windows/http/diskboss_get_bof	2016-12-05	excellent	This module exploits a stack-based buffer overflow vulnerability in the web interface c DiskBoss Enterprise v7.5.12, v7.4.28, and v8.2.14, caused by improper bounds check of the request path in ... **Platforms**: win **Refs**: source
Disk Sorter Enterprise GET Buffer Overflow exploit/windows/http/disksorter_bof	2017-03-15	great	This module exploits a stack-based buffer overflow vulnerability in the web interface c Disk Sorter Enterprise v9.5.12, caused by improper bounds checking of the request p HTTP GET requests ... **Platforms**: win **CVEs**: CVE-2017-7230 **Refs**: source
Disk Pulse Enterprise Login Buffer Overflow exploit/windows/http/disk_pulse_enterprise_bof	2016-10-03	excellent	This module exploits a stack buffer overflo Disk Pulse Enterprise 9.0.34. If a malicious sends a malicious HTTP login request, it is possible to execute a payload that would ru under the ... **Platforms**: win **Refs**: source
Disk Pulse Enterprise GET Buffer Overflow exploit/windows/http/disk_pulse_enterprise_get	2017-08-25	excellent	This module exploits an SEH buffer overflo Disk Pulse Enterprise 9.9.16. If a malicious sends a crafted HTTP GET request it is po to execute a payload that would run under Windows ... **Platforms**: win **Refs**: source
D-Link Central WiFi Manager CWM(100) RCE exploit/windows/http/dlink_central_wifimanager_rce	2019-07-09	excellent	This module exploits a PHP code injection vulnerability in D-Link Central WiFi Manage CWM(100) versions below `v1.03R0100_BETA6`. The vulnerability ex the username cookie, which is passed to .. **Platforms**: php **CVEs**: CVE-2019-13372 **Refs**: source, ref1
DotNetNuke Cookie Deserialization Remote Code Excecution exploit/windows/http/dnn_cookie_deserialization_rce	2017-07-20	excellent	This module exploits a deserialization vulnerability in DotNetNuke (DNN) versions 5.0.0 to 9.3.0-RC. Vulnerable versions stor profile information for users in the DNNPersonalization cookie as XML. ... **Platforms**: win **CVEs**: CVE-2017-9822, CVE-2018-15811, CVE-2018-15812, CVE-2018-18325, CVE-2018-18326 **Refs**: source, ref1, ref2, ref3
Dup Scout Enterprise GET Buffer Overflow exploit/windows/http/dupscts_bof	2017-03-15	great	This module exploits a stack-based buffer overflow vulnerability in the web interface c Dup Scout Enterprise versions <= 10.0.18, caused by improper bounds checking of th request path in HTTP GET ... **Platforms**: win **CVEs**: CVE-2017-13696 **Refs**: source

Metasploit Module	Date	Rank	Details
Dup Scout Enterprise Login Buffer Overflow exploit/windows/http/dup_scout_enterprise_login_bof	2017-11-14	great	This module exploits a stack buffer overflo Dup Scout Enterprise versions <= 10.0.18. buffer overflow exists via the web interface during login. This gives NT AUTHORITYSYSTEM access. This ... **Platforms**: win **CVEs**: CVE-2017-13696 **Refs**: source
Easy Chat Server User Registeration Buffer Overflow (SEH) exploit/windows/http/easychatserver_seh	2017-10-09	normal	This module exploits a buffer overflow duri user registration in Easy Chat Server softw **Platforms**: win **Refs**: source
Easy File Sharing HTTP Server 7.2 POST Buffer Overflow exploit/windows/http/easyfilesharing_post	2017-06-12	normal	This module exploits a POST buffer overflo the Easy File Sharing FTP Server 7.2 softv **Platforms**: win **Refs**: source
Easy File Sharing HTTP Server 7.2 SEH Overflow exploit/windows/http/easyfilesharing_seh	2015-12-02	normal	This module exploits a SEH overflow in the Easy File Sharing FTP Server 7.2 software **Platforms**: win **Refs**: source
EasyFTP Server list.html path Stack Buffer Overflow exploit/windows/http/easyftp_list	2010-02-18	great	This module exploits a stack-based buffer overflow in EasyFTP Server 1.7.0.11 and e EasyFTP fails to check input size when pa the 'path' parameter supplied to an HTTP G request, which ... **Platforms**: win **Refs**: source
Novell eDirectory NDS Server Host Header Overflow exploit/windows/http/edirectory_host	2006-10-21	great	This module exploits a stack buffer overflo Novell eDirectory 8.8.1. The web interface not validate the length of the HTTP Host he prior to using the value of that header in ar HTTP ... **Platforms**: win **CVEs**: CVE-2006-5478 **Refs**: source
eDirectory 8.7.3 iMonitor Remote Stack Buffer Overflow exploit/windows/http/edirectory_imonitor	2005-08-11	great	This module exploits a stack buffer overflo eDirectory 8.7.3 iMonitor service. This vulnerability was discovered by Peter Wint Smith of NGSSoftware. NOTE: repeated exploitation attempts may ... **Platforms**: win **CVEs**: CVE-2005-2551 **Refs**: source
EFS Easy Chat Server Authentication Request Handling Buffer Overflow exploit/windows/http/efs_easychatserver_username	2007-08-14	great	This module exploits a stack buffer overflo EFS Software Easy Chat Server versions 2 3.1. By sending an overly long authenticati request, an attacker may be able to execut arbitrary code. **Platforms**: win **CVEs**: CVE-2004-2466 **Refs**: source
Easy File Management Web Server Stack Buffer Overflow exploit/windows/http/efs_fmws_userid_bof	2014-05-20	normal	Easy File Management Web Server v4.0 a v5.3 contains a stack buffer overflow condi that is triggered as user-supplied input is n properly validated when handling the User cookie. This may ... **Platforms**: win **CVEs**: CVE-2014-3791 **Refs**: source, ref1, ref2
Ektron 8.5, 8.7, 9.0 XSLT Transform Remote Code Execution exploit/windows/http/ektron_xslt_exec_ws	2015-02-05	excellent	Ektron 8.5, 8.7 <= sp1, 9.0 < sp1 have vulnerabilities in various operations within t ServerControlWS.asmx web services. The vulnerabilities allow for RCE without authentication and execute in ... **Platforms**: win **CVEs**: CVE-2015-0923 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Ericom AccessNow Server Buffer Overflow exploit/windows/http/ericom_access_now_bof	2014-06-02	normal	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 ca triggered with a ... **Platforms**: win **CVEs**: CVE-2014-3913 **Refs**: source, ref1
Microsoft Exchange Server DlpUtils AddTenantDlpPolicy RCE exploit/windows/http/exchange_ecp_dlp_policy	2021-01-12	excellent	This vulnerability allows remote attackers t execute arbitrary code on affected installat of Exchange Server. Authentication is requ to exploit this vulnerability. Additionally, the target ... **Platforms**: win **CVEs**: CVE-2020-16875, CVE-2020-1713 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7
Exchange Control Panel ViewState Deserialization exploit/windows/http/exchange_ecp_viewstate	2020-02-11	excellent	This module exploits a .NET serialization vulnerability in the Exchange Control Pane (ECP) web page. The vulnerability is due t Microsoft Exchange Server not randomizin keys on a ... **Platforms**: win **CVEs**: CVE-2020-0688 **Refs**: source, ref1
Microsoft Exchange ProxyLogon RCE exploit/windows/http/exchange_proxylogon_rce	2021-03-02	excellent	This module exploit a vulnerability on Micr Exchange Server that allows an attacker bypassing the authentication, impersonatin the admin (CVE-2021-26855) and write arb file ... **Platforms**: win **CVEs**: CVE-2021-26855, CVE-2021-2706 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref
EZHomeTech EzServer Stack Buffer Overflow Vulnerability exploit/windows/http/ezserver_http	2012-06-18	excellent	This module exploits a stack buffer overflo the EZHomeTech EZServer for versions 6. and earlier. If a malicious user sends packe containing an overly long string, it may be possible to ... **Platforms**: win **Refs**: source, ref1
Free Download Manager Remote Control Server Buffer Overflow exploit/windows/http/fdm_auth_header	2009-02-02	great	This module exploits a stack buffer overflo Free Download Manager Remote Control 2 Build 758. When sending a specially crafte Authorization header, an attacker may be a to execute arbitrary ... **Platforms**: win **CVEs**: CVE-2009-0183 **Refs**: source
File Sharing Wizard - POST SEH Overflow exploit/windows/http/file_sharing_wizard_seh	2019-09-24	normal	This module exploits an unauthenticated H POST SEH-based buffer overflow in File Sharing Wizard 1.5.0. **Platforms**: win **Refs**: source
FlexDotnetCMS Arbitrary ASP File Upload exploit/windows/http/flexdotnetcms_upload_exec	2020-09-28	excellent	This module exploits an arbitrary file uploa vulnerability in FlexDotnetCMS v1.5.8 and in order to execute arbitrary commands wit elevated privileges. The module first tries t authenticate ... **Platforms**: win **CVEs**: CVE-2020-27386 **Refs**: source
FortiLogger Arbitrary File Upload Exploit exploit/windows/http/fortilogger_arbitrary_fileupload	2021-02-26	normal	This module exploits an unauthenticated arbitrary file upload via insecure POST req It has been tested on versions < 5.2.0 in Windows 10 Enterprise. **Platforms**: win **CVEs**: CVE-2021-3378 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Generic Web Application DLL Injection exploit/windows/http/generic_http_dll_injection	2015-03-04	manual	This is a general-purpose module for explo conditions where a HTTP request triggers load from an specified SMB share. This mo serves payloads as DLLs over an SMB ser and allows an ... **Platforms**: win **Refs**: source
Geutebrueck GCore - GCoreServer.exe Buffer Overflow RCE exploit/windows/http/geutebrueck_gcore_x64_rce_bo	2017-01-24	normal	This module exploits a stack Buffer Overflo the GCore server (GCoreServer.exe). The vulnerable webserver is running on Port 13 and Port 13004, does not require authentic and affects all ... **Platforms**: win **CVEs**: CVE-2017-11517 **Refs**: source
GitStack Unsanitized Argument RCE exploit/windows/http/gitstack_rce	2018-01-15	great	This module exploits a remote code execut vulnerability that exists in GitStack through v2.3.10, caused by an unsanitized argume being passed to an exec function call. This module has been ... **Platforms**: win **CVEs**: CVE-2018-5955 **Refs**: source, ref1
HPE Systems Insight Manager AMF Deserialization RCE exploit/windows/http/hpe_sim_76_amf_deserialization	2020-12-15	excellent	A remotely exploitable vulnerability exists v HPE System Insight Manager (SIM) versio 7.6.x that can be leveraged by a remote unauthenticated attacker to execute code v the context of HPE ... **Platforms**: win **CVEs**: CVE-2020-7200 **Refs**: source, ref1, ref2, ref3
HP AutoPass License Server File Upload exploit/windows/http/hp_autopass_license_traversal	2014-01-10	great	This module exploits a code execution flaw HP AutoPass License Server. It abuses tw weaknesses in order to get its objective. Fi the AutoPass application doesn't enforce authentication in the ... **Platforms**: java **CVEs**: CVE-2013-6221 **Refs**: source, ref1
Oracle Weblogic Apache Connector POST Request Buffer Overflow exploit/windows/http/bea_weblogic_post_bof	2008-07-17	great	This module exploits a stack based buffer overflow in the BEA Weblogic Apache plug The connector fails to properly handle spec crafted HTTP POST requests, resulting a b overflow due to ... **Platforms**: win **CVEs**: CVE-2008-3257 **Refs**: source
DiskSavvy Enterprise GET Buffer Overflow exploit/windows/http/disksavvy_get_bof	2016-12-01	excellent	This module exploits a stack-based buffer overflow vulnerability in the web interface c DiskSavvy Enterprise v9.1.14 and v9.3.14, caused by improper bounds checking of th request path in HTTP GET ... **Platforms**: win **CVEs**: CVE-2017-6187 **Refs**: source
Ektron 8.02 XSLT Transform Remote Code Execution exploit/windows/http/ektron_xslt_exec	2012-10-16	excellent	This module exploits a vulnerability in Ektro CMS 8.02 (before SP5). The vulnerability e due to the insecure usage of XslCompiledTransform, using a XSLT cont by the user. The module has ... **Platforms**: win **CVEs**: CVE-1012-5358, CVE-2012-5357 **Refs**: source, ref1, ref2
HP Intelligent Management Center BIMS UploadServlet Directory Traversal exploit/windows/http/hp_imc_bims_upload	2013-10-08	excellent	This module exploits a directory traversal vulnerability on the version 5.2 of the BIMS component from the HP Intelligent Manage Center. The vulnerability exists in the UploadServlet, allowing ... **Platforms**: win **CVEs**: CVE-2013-4822 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
HP OpenView Network Node Manager ovwebsnmpsrv.exe main Buffer Overflow exploit/windows/http/hp_nnm_ovwebsnmpsrv_main	2010-06-16	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 prior to NNM_01203. By specifying a long parameter when executing the 'jovgraph.ex CGI program, an ... **Platforms**: win **CVEs**: CVE-2010-1961, CVE-2010-1964 **Refs**: source
HP SiteScope Remote Code Execution exploit/windows/http/hp_sitescope_runomagentcommand	2013-07-29	manual	This module exploits a code execution flaw HP SiteScope. The vulnerability exists in th opcactivate.vbs script, which is reachable f the APIBSMIntegrationImpl AXIS service, a uses ... **Platforms**: win **CVEs**: CVE-2013-2367 **Refs**: source
Kentico CMS Staging SyncServer Unserialize Remote Command Execution exploit/windows/http/kentico_staging_syncserver	2019-04-15	excellent	This module exploits a vulnerability in the Kentico CMS platform versions 12.0.14 an earlier. Remote Command Execution is pos via unauthenticated XML requests to the Staging Service ... **Platforms**: win **CVEs**: CVE-2019-10068 **Refs**: source, ref1
MiniWeb (Build 300) Arbitrary File Upload exploit/windows/http/miniweb_upload_wbem	2013-04-09	excellent	This module exploits a vulnerability in MiniW HTTP server (build 300). The software con a file upload vulnerability that allows an unauthenticated remote attacker to write arbitrary files to ... **Platforms**: win **Refs**: source
Oracle Secure Backup Authentication Bypass/Command Injection Vulnerability exploit/windows/http/osb_uname_jlist	2010-07-13	excellent	This module exploits an authentication byp vulnerability in login.php. In conjunction wit authentication bypass issue, the 'jlist' paran in property_box.php can be used to execut **Platforms**: win **CVEs**: CVE-2010-0904 **Refs**: source
Serviio Media Server checkStreamUrl Command Execution exploit/windows/http/serviio_checkstreamurl_cmd_exec	2017-05-03	excellent	This module exploits an unauthenticated re command execution vulnerability in the cor component of Serviio Media Server versior to 1.8 on Windows operating systems. The console service ... **Platforms**: win **Refs**: source, ref1, ref2
Telerik UI ASP.NET AJAX RadAsyncUpload Deserialization exploit/windows/http/telerik_rau_deserialization	2019-12-09	excellent	This module exploits the .NET deserializati vulnerability within the RadAsyncUpload (R component of Telerik UI ASP.NET AJAX th identified as CVE-2019-18935. In order to the module ... **Platforms**: win **CVEs**: CVE-2017-11317, CVE-2019-1893 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7
HP Intelligent Management Java Deserialization RCE exploit/windows/http/hp_imc_java_deserialize	2017-10-03	excellent	This vulnerability allows remote attackers t execute arbitrary code on vulnerable installations of Hewlett Packard Enterprise Intelligent Management Center. Authentica is not required to exploit ... **Platforms**: win **CVEs**: CVE-2017-12557 **Refs**: source, ref1, ref2
HP Intelligent Management Center Arbitrary File Upload exploit/windows/http/hp_imc_mibfileupload	2013-03-07	great	This module exploits a code execution flaw HP Intelligent Management Center. The vulnerability exists in the mibFileUpload wh accepting unauthenticated file uploads and handling zip contents ... **Platforms**: win **CVEs**: CVE-2012-5201 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
HP LoadRunner EmulationAdmin Web Service Directory Traversal exploit/windows/http/hp_loadrunner_copyfiletoserver	2013-10-30	excellent	This module exploits a directory traversal vulnerability in version 11.52 of HP LoadRu The vulnerability exists in the EmulationAd web service, specifically in the copyFileToS method, ... **Platforms**: win **CVEs**: CVE-2013-4837 **Refs**: source, ref1
HP Managed Printing Administration jobAcct Remote Command Execution exploit/windows/http/hp_mpa_job_acct	2011-12-21	excellent	This module exploits an arbitrary file uploa vulnerability on HP Managed Printing Administration 2.6.3 and prior versions. Th vulnerability exists in the UploadFiles() fun from the ... **Platforms**: win **CVEs**: CVE-2011-4166 **Refs**: source, ref1
HP OpenView Network Node Manager getnnmdata.exe (Hostname) CGI Buffer Overflow exploit/windows/http/hp_nnm_getnnmdata_hostname	2010-05-11	great	This module exploits a buffer overflow in H OpenView Network Node Manager 7.50/7. By sending specially crafted Hostname parameter to the getnnmdata.exe CGI, an attacker may be able to execute ... **Platforms**: win **CVEs**: CVE-2010-1555 **Refs**: source
HP OpenView Network Node Manager getnnmdata.exe (ICount) CGI Buffer Overflow exploit/windows/http/hp_nnm_getnnmdata_icount	2010-05-11	great	This module exploits a buffer overflow in H OpenView Network Node Manager 7.50/7. By sending specially crafted ICount param to the getnnmdata.exe CGI, an attacker ma able to execute ... **Platforms**: win **CVEs**: CVE-2010-1554 **Refs**: source
HP OpenView Network Node Manager getnnmdata.exe (MaxAge) CGI Buffer Overflow exploit/windows/http/hp_nnm_getnnmdata_maxage	2010-05-11	great	This module exploits a buffer overflow in H OpenView Network Node Manager 7.50/7. By sending specially crafted MaxAge para to the getnnmdata.exe CGI, an attacker ma able to execute ... **Platforms**: win **CVEs**: CVE-2010-1553 **Refs**: source
HP OpenView NNM nnmRptConfig nameParams Buffer Overflow exploit/windows/http/hp_nnm_nnmrptconfig_nameparams	2011-01-10	normal	This module exploits a vulnerability in HP NNM's nnmRptConfig.exe. A remote user send a long string data to the nameParams parameter via a POST request, which caus an overflow on the stack when ... **Platforms**: win **CVEs**: CVE-2011-0266 **Refs**: source
HP OpenView NNM nnmRptConfig.exe schdParams Buffer Overflow exploit/windows/http/hp_nnm_nnmrptconfig_schdparams	2011-01-10	normal	This module exploits NNM's nnmRptConfig Similar to other NNM CGI bugs, the overflo occurs during a ov.sprintf_new() call, which allows an attacker to overwrite data on the stack, and gain ... **Platforms**: win **CVEs**: CVE-2011-0267 **Refs**: source
HP OpenView Network Node Manager OpenView5.exe CGI Buffer Overflow exploit/windows/http/hp_nnm_openview5	2007-12-06	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 sending a specially crafted CGI request, ar attacker may be able to execute arbitrary c **Platforms**: win **CVEs**: CVE-2007-6204 **Refs**: source
HP OpenView Network Node Manager ovalarm.exe CGI Buffer Overflow exploit/windows/http/hp_nnm_ovalarm_lang	2009-12-09	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 sending a specially crafted CGI request to ovalarm.exe, an attacker can execute arbit code. This specific ... **Platforms**: win **CVEs**: CVE-2009-4179 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
HP OpenView NNM 7.53, 7.51 OVAS.EXE Pre-Authentication Stack Buffer Overflow exploit/windows/http/hp_nnm_ovas	2008-04-02	good	This module exploits a stack buffer overflo HP OpenView Network Node Manager ver 7.53 and earlier. Specifically this vulnerabil caused by a failure to properly handle user supplied ... **Platforms**: win **CVEs**: CVE-2008-1697 **Refs**: source
HP OpenView Network Node Manager ov.dll _OVBuildPath Buffer Overflow exploit/windows/http/hp_nnm_ovbuildpath_textfile	2011-11-01	normal	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 prior to NNM_01213 without the SSRT100 hotfix. By specifying a long 'textFile' argum when calling the ... **Platforms**: win **CVEs**: CVE-2011-3167 **Refs**: source, ref1
HP OpenView Network Node Manager OvWebHelp.exe CGI Buffer Overflow exploit/windows/http/hp_nnm_ovwebhelp	2009-12-09	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 sending a specially crafted CGI request to OvWebHelp.exe, an attacker may be able execute arbitrary code. **Platforms**: win **CVEs**: CVE-2009-4178 **Refs**: source
HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil Buffer Overflow exploit/windows/http/hp_nnm_ovwebsnmpsrv_ovutil	2010-06-16	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 prior to NNM_01203. By specifying a long parameter when executing the 'jovgraph.ex CGI program, an ... **Platforms**: win **CVEs**: CVE-2010-1961, CVE-2010-1964 **Refs**: source, ref1
HP OpenView Network Node Manager ovwebsnmpsrv.exe Unrecognized Option Buffer Overflow exploit/windows/http/hp_nnm_ovwebsnmpsrv_uro	2010-06-08	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 prior to NNM_01203. By specifying a long parameter when executing the 'jovgraph.ex CGI program, an ... **Platforms**: win **CVEs**: CVE-2010-1960 **Refs**: source
HP OpenView Network Node Manager Snmp.exe CGI Buffer Overflow exploit/windows/http/hp_nnm_snmp	2009-12-09	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 sending a specially crafted CGI request to Snmp.exe, an attacker may be able to exe arbitrary code. **Platforms**: win **CVEs**: CVE-2009-3849 **Refs**: source
HP OpenView Network Node Manager snmpviewer.exe Buffer Overflow exploit/windows/http/hp_nnm_snmpviewer_actapp	2010-05-11	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 prior to NNM_01203. By making a specially crafted HTTP request to the "snmpviewer.e CGI program, an attacker ... **Platforms**: win **CVEs**: CVE-2010-1552 **Refs**: source, ref1
HP OpenView Network Node Manager Toolbar.exe CGI Buffer Overflow exploit/windows/http/hp_nnm_toolbar_01	2009-01-07	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 sending a specially crafted CGI request to Toolbar.exe, an attacker may be able to ex arbitrary code. **Platforms**: win **CVEs**: CVE-2008-0067 **Refs**: source
HP OpenView Network Node Manager Toolbar.exe CGI Cookie Handling Buffer Overflow exploit/windows/http/hp_nnm_toolbar_02	2009-01-21	normal	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.0 7.53. By sending a CGI request with a spe OvOSLocale cookie to Toolbar.exe, an atta may be able to ... **Platforms**: win **CVEs**: CVE-2009-0920 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
HP OpenView Network Node Manager execvp_nc Buffer Overflow exploit/windows/http/hp_nnm_webappmon_execvp	2010-07-20	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 prior to NNM_01207 or NNM_01206 witho SSRT100025 hotfix. By specifying a long 's parameter when calling ... **Platforms**: win **CVEs**: CVE-2010-2703 **Refs**: source, ref1
HP NNM CGI webappmon.exe OvJavaLocale Buffer Overflow exploit/windows/http/hp_nnm_webappmon_ovjavalocale	2010-08-03	great	This module exploits a stack buffer overflo HP OpenView Network Node Manager 7.5 sending a request containing a cookie long than 5120 bytes, an attacker can overflow stack buffer and ... **Platforms**: win **CVEs**: CVE-2010-2709 **Refs**: source, ref1, ref2
HP OpenView Performance Insight Server Backdoor Account Code Execution exploit/windows/http/hp_openview_insight_backdoor	2011-01-31	excellent	This module exploits a hidden account in th com.trinagy.security.XMLUserManager Jav class. When using this account, an attacke abuse the com.trinagy.servlet.HelpManagerServlet cl and write ... **Platforms**: win **CVEs**: CVE-2011-0276 **Refs**: source
HP ProCurve Manager SNAC UpdateCertificatesServlet File Upload exploit/windows/http/hp_pcm_snac_update_certificates	2013-09-09	excellent	This module exploits a path traversal flaw i HP ProCurve Manager SNAC Server. The vulnerability in the UpdateCertificatesServl allows an attacker to upload arbitrary files, having into ... **Platforms**: win **CVEs**: CVE-2013-4812 **Refs**: source
HP ProCurve Manager SNAC UpdateDomainControllerServlet File Upload exploit/windows/http/hp_pcm_snac_update_domain	2013-09-09	excellent	This module exploits a path traversal flaw i HP ProCurve Manager SNAC Server. The vulnerability in the UpdateDomainControllerServlet allows an attacker to upload arbitrary files, just havin **Platforms**: win **CVEs**: CVE-2013-4811 **Refs**: source
HP Power Manager 'formExportDataLogs' Buffer Overflow exploit/windows/http/hp_power_manager_filename	2011-10-19	normal	This module exploits a buffer overflow in H Power Manager's 'formExportDataLogs'. B creating a malformed request specifically f fileName parameter, a stack-based buffer overflow occurs due to ... **Platforms**: win **CVEs**: CVE-2009-3999 **Refs**: source
Hewlett-Packard Power Manager Administration Buffer Overflow exploit/windows/http/hp_power_manager_login	2009-11-04	average	This module exploits a stack buffer overflo Hewlett-Packard Power Manager 4.2. Sen specially crafted POST request with an ov long Login string, an attacker may be able execute ... **Platforms**: win **CVEs**: CVE-2009-2685 **Refs**: source
HP SiteScope DNS Tool Command Injection exploit/windows/http/hp_sitescope_dns_tool	2015-10-09	good	This module exploits a command injection vulnerability discovered in HP SiteScope 1 and earlier versions (tested in 11.26 and 11 The vulnerability exists in the DNS Tool all an attacker ... **Platforms**: win **Refs**: source, ref1, ref2
HTTPDX h_handlepeer() Function Buffer Overflow exploit/windows/http/httpdx_handlepeer	2009-10-08	great	This module exploits a stack-based buffer overflow vulnerability in HTTPDX HTTP se 1.4. The vulnerability is caused due to a boundary error within the "h_handlepeer()" function in http.cpp. By ... **Platforms**: win **CVEs**: CVE-2009-3711 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
HTTPDX tolog() Function Format String Vulnerability exploit/windows/http/httpdx_tolog_format	2009-11-17	great	This module exploits a format string vulner in HTTPDX HTTP server. By sending a spe crafted HTTP request containing format specifiers, an attacker can corrupt memory execute ... **Platforms**: win **CVEs**: CVE-2009-4769 **Refs**: source
IA WebMail 3.x Buffer Overflow exploit/windows/http/ia_webmail	2003-11-03	average	This exploits a stack buffer overflow in the WebMail server. This exploit has not been tested against a live system at this time. **Platforms**: win **CVEs**: CVE-2003-1192 **Refs**: source, ref1
IBM Tivoli Endpoint Manager POST Query Buffer Overflow exploit/windows/http/ibm_tivoli_endpoint_bof	2011-05-31	good	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 ... **Platforms**: win **CVEs**: CVE-2011-1220 **Refs**: source
IBM TPM for OS Deployment 5.1.0.x rembo.exe Buffer Overflow exploit/windows/http/ibm_tpmfosd_overflow	2007-05-02	good	This is a stack buffer overflow exploit for IB Tivoli Provisioning Manager for OS Deploy version 5.1.0.X. **Platforms**: win **CVEs**: CVE-2007-1868 **Refs**: source, ref1
IBM Tivoli Storage Manager Express CAD Service Buffer Overflow exploit/windows/http/ibm_tsm_cad_header	2007-09-24	good	This module exploits a stack buffer overflo the IBM Tivoli Storage Manager Express C Service (5.3.3). By sending an overly long request, it may be possible for an attacker execute ... **Platforms**: win **CVEs**: CVE-2007-4880 **Refs**: source
Icecast Header Overwrite exploit/windows/http/icecast_header	2004-09-28	great	This module exploits a buffer overflow in th header parsing of icecast versions 2.0.1 ar earlier, discovered by Luigi Auriemma. Ser 32 HTTP headers will cause a write one pa the end of a ... **Platforms**: win **CVEs**: CVE-2004-1561 **Refs**: source, ref1
Race River Integard Home/Pro LoginAdmin Password Stack Buffer Overflow exploit/windows/http/integard_password_bof	2010-09-07	great	This module exploits a stack buffer overflo Race river's Integard Home/Pro internet co filter HTTP Server. Versions prior to 2.0.0.9 and 2.2.0.9037 are vulnerable. The administration web ... **Platforms**: win **Refs**: source, ref1
InterSystems Cache UtilConfigHome.csp Argument Buffer Overflow exploit/windows/http/intersystems_cache	2009-09-29	great	This module exploits a stack buffer overflo InterSystems Cache 2009.1. By sending a specially crafted GET request, an attacker be able to execute arbitrary code. **Platforms**: win **Refs**: source
Intrasrv 1.0 Buffer Overflow exploit/windows/http/intrasrv_bof	2013-05-30	manual	This module exploits a boundary condition in Intrasrv Simple Web Server 1.0. The we interface does not validate the boundaries HTTP request string prior to copying the da an ... **Platforms**: win **Refs**: source
Ipswitch WhatsUp Gold 8.03 Buffer Overflow exploit/windows/http/ipswitch_wug_maincfgret	2004-08-25	great	This module exploits a buffer overflow in IPswitch WhatsUp Gold 8.03. By posting a string for the value of 'instancename' in the _maincfgret.cgi script an attacker can over buffer and ... **Platforms**: win **CVEs**: CVE-2004-0798 **Refs**: source

Metasploit Module	Date	Rank	Details
JIRA Issues Collector Directory Traversal exploit/windows/http/jira_collector_traversal	2014-02-26	normal	This module exploits a directory traversal f JIRA 6.0.3. The vulnerability exists in the is collector code, while handling attachments provided by the user. It can be exploited in Windows ... **Platforms**: win **CVEs**: CVE-2014-2314 **Refs**: source, ref1, ref2
Kaseya VSA uploader.aspx Arbitrary File Upload exploit/windows/http/kaseya_uploader	2015-09-23	excellent	This module exploits an arbitrary file uploa vulnerability found in Kaseya VSA versions between 7 and 9.1. A malicious unauthenti user can upload an ASP file to an arbitrary directory leading ... **Platforms**: win **CVEs**: CVE-2015-6922 **Refs**: source, ref1, ref2
Kaseya uploadImage Arbitrary File Upload exploit/windows/http/kaseya_uploadimage_file_upload	2013-11-11	excellent	This module exploits an arbitrary file uploa vulnerability found in Kaseya versions belo 6.3.0.2. A malicious user can upload an AS to an arbitrary directory without previous authentication, ... **Platforms**: win **Refs**: source, ref1
Kolibri HTTP Server HEAD Buffer Overflow exploit/windows/http/kolibri_http	2010-12-26	good	This exploits a stack buffer overflow in vers of the Kolibri HTTP server. **Platforms**: win **CVEs**: CVE-2002-2268 **Refs**: source
LANDesk Lenovo ThinkManagement Console Remote Command Execution exploit/windows/http/landesk_thinkmanagement_upload_asp	2012-02-15	excellent	This module can be used to execute a pay on LANDesk Lenovo ThinkManagement Su 9.0.2 and 9.0.3. The payload is uploaded a ASP script by sending a specially crafted S request to ... **Platforms**: win **CVEs**: CVE-2012-1195, CVE-2012-1196 **Refs**: source
Lexmark MarkVision Enterprise Arbitrary File Upload exploit/windows/http/lexmark_markvision_gfd_upload	2014-12-09	excellent	This module exploits a code execution flaw Lexmark MarkVision Enterprise before vers 2.1. A directory traversal vulnerability in the GfdFileUploadServlet servlet allows an unauthenticated ... **Platforms**: win **CVEs**: CVE-2014-8741 **Refs**: source, ref1
MailEnable Authorization Header Buffer Overflow exploit/windows/http/mailenable_auth_header	2005-04-24	great	This module exploits a remote buffer overfl the MailEnable web service. The vulnerabi triggered when a large value is placed into Authorization header of the web request. MailEnable ... **Platforms**: win **CVEs**: CVE-2005-1348 **Refs**: source, ref1
Manage Engine Exchange Reporter Plus Unauthenticated RCE exploit/windows/http/manageengine_adshacluster_rce	2018-06-28	excellent	This module exploits a remote code execut vulnerability that exists in Exchange Repor Plus <= 5310, caused by execution of bcp. file inside ADSHACluster servlet. **Platforms**: win **Refs**: source, ref1
ManageEngine Applications Manager Remote Code Execution exploit/windows/http/manageengine_appmanager_exec	2018-03-07	excellent	This module exploits command injection vulnerability in the ManageEngine Applicat Manager product. An unauthenticated user execute a operating system command und context of privileged ... **Platforms**: win **CVEs**: CVE-2018-7890 **Refs**: source, ref1, ref2
ManageEngine Applications Manager Authenticated Code Execution exploit/windows/http/manageengine_apps_mngr	2011-04-08	average	This module logs into the Manage Engine Applications Manager to upload a payload file system and a batch script that executes payload. **Platforms**: win **Refs**: source

Metasploit Module	Date	Rank	Details
ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability exploit/windows/http/manageengine_connectionid_write	2015-12-14	excellent	This module exploits a vulnerability found i ManageEngine Desktop Central 9. When uploading a 7z file, the FileUploadServlet c does not check the user-controlled ConnectionId parameter in the ... **Platforms**: win **CVEs**: CVE-2015-8249 **Refs**: source, ref1
ManageEngine OpManager Remote Code Execution exploit/windows/http/manage_engine_opmanager_rce	2015-09-14	manual	This module exploits a default credential vulnerability in ManageEngine OpManager where a default hidden account "IntegrationUser" with administrator privileg exists. The account has a default ... **Platforms**: java **CVEs**: CVE-2015-7765, CVE-2015-7766 **Refs**: source, ref1, ref2
MaxDB WebDBM Database Parameter Overflow exploit/windows/http/maxdb_webdbm_database	2006-08-29	good	This module exploits a stack buffer overflo the MaxDB WebDBM service. By sending specially-crafted HTTP request that contai overly long database name. A remote attac could overflow a ... **Platforms**: win **CVEs**: CVE-2006-4305 **Refs**: source
MaxDB WebDBM GET Buffer Overflow exploit/windows/http/maxdb_webdbm_get_overflow	2005-04-26	good	This module exploits a stack buffer overflo the MaxDB WebDBM service. This service included with many recent versions of the MaxDB and SAPDB products. This particu module is capable of ... **Platforms**: win **CVEs**: CVE-2005-0684 **Refs**: source, ref1
McAfee ePolicy Orchestrator / ProtectionPilot Overflow exploit/windows/http/mcafee_epolicy_source	2006-07-17	average	This is an exploit for the McAfee HTTP Ser (NAISERV.exe). McAfee ePolicy Orchestra 2.5.1 <= 3.5.0 and ProtectionPilot 1.1.0 are known to be vulnerable. By sending a large 'Source' header, the ... **Platforms**: win **CVEs**: CVE-2006-5156 **Refs**: source
MDaemon WorldClient form2raw.cgi Stack Buffer Overflow exploit/windows/http/mdaemon_worldclient_form2raw	2003-12-29	great	This module exploits a stack buffer overflo Alt-N MDaemon SMTP server for versions and earlier. When WorldClient HTTP serve installed (default a CGI script is provided to accept html ... **Platforms**: win **CVEs**: CVE-2003-1200 **Refs**: source
Minishare 1.4.1 Buffer Overflow exploit/windows/http/minishare_get_overflow	2004-11-07	average	This is a simple buffer overflow for the min web server. This flaw affects all versions pr 1.4.2. This is a plain stack buffer overflow t requires a "jmp esp" to reach the payload, **Platforms**: win **CVEs**: CVE-2004-2271 **Refs**: source, ref1
NaviCOPA 2.0.1 URL Handling Buffer Overflow exploit/windows/http/navicopa_get_overflow	2006-09-28	great	This module exploits a stack buffer overflo NaviCOPA 2.0.1. The vulnerability is cause due to a boundary error within the handling URL parameters. **Platforms**: win **CVEs**: CVE-2006-5112 **Refs**: source
NetDecision 4.5.1 HTTP Server Buffer Overflow exploit/windows/http/netdecision_http_bof	2012-02-24	normal	This module exploits a vulnerability found i NetDecision's HTTP service (located in C:Program FilesNetDecisionBinHttpSvr.ex supplying a long string of data to the URL, overflow may occur if ... **Platforms**: win **CVEs**: CVE-2012-1465 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
NETGEAR ProSafe Network Management System 300 Arbitrary File Upload exploit/windows/http/netgear_nms_rce	2016-02-04	excellent	Netgear's ProSafe NMS300 is a network management utility that runs on Windows systems. The application has a file upload vulnerability that can be exploited by an unauthenticated remote attacker to ... **Platforms**: win **CVEs**: CVE-2016-1525 **Refs**: source, ref1, ref2
Novell iManager getMultiPartParameters Arbitrary File Upload exploit/windows/http/novell_imanager_upload	2010-10-01	excellent	This module exploits a directory traversal vulnerability which allows remote attackers upload and execute arbitrary code. PortalModuleInstallManager. **Platforms**: win **Refs**: source, ref1
Novell Zenworks Mobile Managment MDM.php Local File Inclusion Vulnerability exploit/windows/http/novell_mdm_lfi	-	excellent	This module exercises a vulnerability in No Zenworks Mobile Management's Mobile De Management component which can allow unauthenticated remote code execution. D a flaw in the MDM.php ... **Platforms**: win **CVEs**: CVE-2013-1081 **Refs**: source, ref1
Novell Messenger Server 2.0 Accept-Language Overflow exploit/windows/http/novell_messenger_acceptlang	2006-04-13	average	This module exploits a stack buffer overflo Novell GroupWise Messenger Server v2.0. flaw is triggered by any HTTP request with Accept-Language header greater than 16 b To overwrite ... **Platforms**: win **CVEs**: CVE-2006-0992 **Refs**: source
Now SMS/MMS Gateway Buffer Overflow exploit/windows/http/nowsms	2008-02-19	good	This module exploits a stack buffer overflo Now SMS/MMS Gateway v2007.06.27. By sending a specially crafted GET request, a attacker may be able to execute arbitrary c **Platforms**: win **CVEs**: CVE-2008-0871 **Refs**: source
Oracle Application Testing Suite WebLogic Server Administration Console War Deployment exploit/windows/http/oats_weblogic_console	2019-03-13	excellent	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 ... **Platforms**: java **CVEs**: CVE-2007-2699 **Refs**: source
Octopus Deploy Authenticated Code Execution exploit/windows/http/octopusdeploy_deploy	2017-05-15	excellent	This module can be used to execute a pay 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 ... **Platforms**: win **Refs**: source, ref1
Oracle 9i XDB HTTP PASS Overflow (win32) exploit/windows/http/oracle9i_xdb_pass	2003-08-18	great	This module exploits a stack buffer overflo the authorization code of the Oracle 9i HTT XDB service. David Litchfield, has illustrate multiple vulnerabilities in the Oracle 9i XML Database ... **Platforms**: win **CVEs**: CVE-2003-0727 **Refs**: source, ref1
Oracle BeeHive 2 voice-servlet processEvaluation() Vulnerability exploit/windows/http/oracle_beehive_evaluation	2010-06-09	excellent	This module exploits a vulnerability found i Oracle BeeHive. The processEvaluation m found in voice-servlet can be abused to wr malicious file onto the target machine, and remote ... **Platforms**: win **CVEs**: CVE-2010-4417 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Oracle BeeHive 2 voice-servlet prepareAudioToPlay() Arbitrary File Upload exploit/windows/http/oracle_beehive_prepareaudiotoplay	2015-11-10	excellent	This module exploits a vulnerability found i Oracle BeeHive. The prepareAudioToPlay method found in voice-servlet can be abus write a malicious file onto the target machir and gain remote ... **Platforms**: win **Refs**: source, ref1
Oracle Business Transaction Management FlashTunnelService Remote Code Execution exploit/windows/http/oracle_btm_writetofile	2012-08-07	excellent	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 meth **Platforms**: java, win **Refs**: source
Oracle Endeca Server Remote Command Execution exploit/windows/http/oracle_endeca_exec	2013-07-16	excellent	This module exploits a command injection vulnerability on the Oracle Endeca Server The vulnerability exists on the createDataS method from the controlSoapBinding web service. The ... **Platforms**: win **CVEs**: CVE-2013-3763 **Refs**: source, ref1
Oracle Event Processing FileUploadServlet Arbitrary File Upload exploit/windows/http/oracle_event_processing_upload	2014-04-21	excellent	This module exploits an arbitrary file uploa vulnerability in Oracle Event Processing 11.1.1.7.0. The FileUploadServlet compone which requires no authentication, can be abused to upload a ... **Platforms**: win **CVEs**: CVE-2014-2424 **Refs**: source, ref1
PeerCast URL Handling Buffer Overflow exploit/windows/http/peercast_url	2006-03-08	average	This module exploits a stack buffer overflo PeerCast <= v0.1216. The vulnerability is caused due to a boundary error within the handling of URL parameters. **Platforms**: win **CVEs**: CVE-2006-1148 **Refs**: source
PHP apache_request_headers Function Buffer Overflow exploit/windows/http/php_apache_request_headers_bof	2012-05-08	normal	This module exploits a stack based buffer overflow in the CGI version of PHP 5.4.x b 5.4.3. The vulnerability is due to the insecu handling of the HTTP headers. This modul been tested ... **Platforms**: win **CVEs**: CVE-2012-2329 **Refs**: source, ref1, ref2, ref3
Plesk/myLittleAdmin ViewState .NET Deserialization exploit/windows/http/plesk_mylittleadmin_viewstate	2020-05-15	excellent	This module exploits a ViewState .NET deserialization vulnerability in web-based M SQL Server management tool myLittleAdm for version 3.8 and likely older versions, du hardcoded ... **Platforms**: win **CVEs**: CVE-2020-13166 **Refs**: source, ref1, ref2
Plex Unpickle Dict Windows RCE exploit/windows/http/plex_unpickle_dict_rce	2020-05-07	normal	This module exploits an authenticated Pyth unsafe pickle.load of a Dict file. An authenticated attacker can create a photo l and add arbitrary files to it. After setting the Windows only Plex ... **Platforms**: python **CVEs**: CVE-2020-5741 **Refs**: source, ref1, ref2, ref3, ref4
Private Wire Gateway Buffer Overflow exploit/windows/http/privatewire_gateway	2006-06-26	average	This exploits a buffer overflow in the ADMCREG.EXE used in the PrivateWire C Registration Facility. **Platforms**: win **CVEs**: CVE-2006-3252 **Refs**: source

Metasploit Module	Date	Rank	Details
PRTG Network Monitor Authenticated RCE exploit/windows/http/prtg_authenticated_rce	2018-06-25	excellent	Notifications can be created by an authenti user and can execute scripts when triggere Due to a poorly validated input on the scrip name, it is possible to chain it with a user-supplied ... **Platforms**: win **CVEs**: CVE-2018-9276 **Refs**: source, ref1
PSO Proxy v0.91 Stack Buffer Overflow exploit/windows/http/psoproxy91_overflow	2004-02-20	average	This module exploits a buffer overflow in th PSO Proxy v0.91 web server. If a client sei an excessively long string the stack is overwritten. **Platforms**: win **CVEs**: CVE-2004-0313 **Refs**: source
RabidHamster R4 Log Entry sprintf() Buffer Overflow exploit/windows/http/rabidhamster_r4_log	2012-02-09	normal	This module exploits a vulnerability found i RabidHamster R4's web server. By supplyi malformed HTTP request, it is possible to trigger a stack-based buffer overflow when generating a log, which ... **Platforms**: win **Refs**: source, ref1, ref2
Rejetto HttpFileServer Remote Command Execution exploit/windows/http/rejetto_hfs_exec	2014-09-11	excellent	Rejetto HttpFileServer (HFS) is vulnerable remote command execution attack due to a poor regex in the file ParserLib.pas. This module exploits the HFS scripting commar using '%00' to bypass ... **Platforms**: win **CVEs**: CVE-2014-6287 **Refs**: source, ref1, ref2
Sambar 6 Search Results Buffer Overflow exploit/windows/http/sambar6_search_results	2003-06-21	normal	This module exploits a buffer overflow four the /search/results.stm application that con with Sambar 6. This code is a direct port of Andrew Griffiths's SMUDGE exploit, the on changes made ... **Platforms**: win **CVEs**: CVE-2004-2086 **Refs**: source
SAP DB 7.4 WebTools Buffer Overflow exploit/windows/http/sapdb_webtools	2007-07-05	great	This module exploits a stack buffer overflo SAP DB 7.4 WebTools. By sending an ove long GET request, it may be possible for a attacker to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2007-3614 **Refs**: source
SAP ConfigServlet Remote Code Execution exploit/windows/http/sap_configservlet_exec_noauth	2012-11-01	great	This module allows remote code execution operating system commands through the S ConfigServlet without any authentication. T module has been tested successfully with S NetWeaver 7.00 and ... **Platforms**: win **Refs**: source, ref1
SAP NetWeaver HostControl Command Injection exploit/windows/http/sap_host_control_cmd_exec	2012-08-14	average	This module exploits a command injection vulnerability in the SAPHostControl Service sending a specially crafted SOAP request t management console. In order to deal with spaces and ... **Platforms**: win **Refs**: source, ref1, ref2
Savant 3.1 Web Server Overflow exploit/windows/http/savant_31_overflow	2002-09-10	great	This module exploits a stack buffer overflo Savant 3.1 Web Server. The service suppo maximum of 10 threads (for a default insta Each exploit attempt generally causes a th to die ... **Platforms**: win **CVEs**: CVE-2002-1120 **Refs**: source

Metasploit Module	Date	Rank	Details
Symantec Endpoint Protection Manager Authentication Bypass and Code Execution exploit/windows/http/sepm_auth_bypass_rce	2015-07-31	excellent	This module exploits three separate vulnerabilities in Symantec Endpoint Prote Manager in order to achieve a remote shel the box as NT AUTHORITYSYSTEM. The vulnerabilities include an ... **Platforms**: win **CVEs**: CVE-2015-1486, CVE-2015-1487, 2015-1489 **Refs**: source, ref1
Rhinosoft Serv-U Session Cookie Buffer Overflow exploit/windows/http/servu_session_cookie	2009-11-01	good	This module exploits a buffer overflow in Rhinosoft Serv-U 9.0.0.5. Sending a specia crafted POST request with an overly long session cookie string, an attacker may be a to execute arbitrary ... **Platforms**: win **CVEs**: CVE-2009-4006 **Refs**: source, ref1
SharePoint DataSet / DataTable Deserialization exploit/windows/http/sharepoint_data_deserialization	2020-07-14	excellent	A remotely exploitable vulnerability exists v SharePoint that can be leveraged by a rem authenticated attacker to execute code witl the context of the SharePoint application service. The ... **Platforms**: win **CVEs**: CVE-2020-1147 **Refs**: source, ref1
Microsoft SharePoint Server-Side Include and ViewState RCE exploit/windows/http/sharepoint_ssi_viewstate	2020-10-13	excellent	This module exploits a server-side include in SharePoint to leak the web.config file an forge a malicious ViewState with the extrac validation key. This exploit is authenticated ... **Platforms**: win **CVEs**: CVE-2020-16952 **Refs**: source, ref1, ref2, ref3
SharePoint Workflows XOML Injection exploit/windows/http/sharepoint_workflows_xoml	2020-03-02	excellent	This module exploits a vulnerability within SharePoint and its .NET backend that allov attacker to execute commands using speci crafted XOML data sent to SharePoint via Workflows ... **Platforms**: win **CVEs**: CVE-2020-0646 **Refs**: source, ref1
SHOUTcast DNAS/win32 1.9.4 File Request Format String Overflow exploit/windows/http/shoutcast_format	2004-12-23	average	This module exploits a format string vulner in the Nullsoft SHOUTcast server for Windo The vulnerability is triggered by requesting path that contains format string specifiers. ... **Platforms**: win **CVEs**: CVE-2004-1373 **Refs**: source
SHTTPD URI-Encoded POST Request Overflow exploit/windows/http/shttpd_post	2006-10-06	average	This module exploits a stack buffer overflo SHTTPD <= 1.34. The vulnerability is caus due to a boundary error within the handling POST requests. Based on an original explo skOd but ... **Platforms**: win **CVEs**: CVE-2006-5216 **Refs**: source, ref1
Solarwinds Firewall Security Manager 6.6.5 Client Session Handling Vulnerability exploit/windows/http/solarwinds_fsm_userlogin	2015-03-13	excellent	This module exploits multiple vulnerabilities found in Solarwinds Firewall Security Mana 6.6.5. The first vulnerability is an authentica bypass via the Change Advisor interface d a ... **Platforms**: win **CVEs**: CVE-2015-2284 **Refs**: source, ref1
Solarwinds Storage Manager 5.1.0 SQL Injection exploit/windows/http/solarwinds_storage_manager_sql	2011-12-07	excellent	This module exploits a SQL injection found Solarwinds Storage Manager login interfac will send a malicious SQL query to create a file under the web root directory, and then l ... **Platforms**: win **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Dell SonicWALL (Plixer) Scrutinizer 9 SQL Injection exploit/windows/http/sonicwall_scrutinizer_sqli	2012-07-22	excellent	This module exploits a vulnerability found i SonicWall Scrutinizer. While handling the 'c parameter, the PHP application does not properly filter the user-supplied data, which be ... **Platforms**: php **CVEs**: CVE-2012-2962 **Refs**: source, ref1
SQL Server Reporting Services (SSRS) ViewState Deserialization exploit/windows/http/ssrs_navcorrector_viewstate	2020-02-11	excellent	A vulnerability exists within Microsoft's SQL Server Reporting Services which can allow attacker to craft an HTTP POST request w serialized object to achieve remote code execution. The ... **Platforms**: win **CVEs**: CVE-2020-0618 **Refs**: source, ref1
Streamcast HTTP User-Agent Buffer Overflow exploit/windows/http/steamcast_useragent	2008-01-24	average	This module exploits a stack buffer overflo Streamcast <= 0.9.75. By sending an overl long User-Agent in an HTTP GET request, attacker may be able to execute arbitrary c **Platforms**: win **CVEs**: CVE-2008-0550 **Refs**: source, ref1
Simple Web Server Connection Header Buffer Overflow exploit/windows/http/sws_connection_bof	2012-07-20	normal	This module exploits a vulnerability in Simp Web Server 2.2 rc2. A remote user can ser long string data in the Connection Header causes an overflow on the stack when func vsprintf() is ... **Platforms**: win **Refs**: source, ref1
Sybase EAServer 5.2 Remote Stack Buffer Overflow exploit/windows/http/sybase_easerver	2005-07-25	average	This module exploits a stack buffer overflo the Sybase EAServer Web Console. The o to the SEH frame appears to change depe on what version of Java is in use by the rer server, making ... **Platforms**: win **CVEs**: CVE-2005-2297 **Refs**: source
Sync Breeze Enterprise GET Buffer Overflow exploit/windows/http/syncbreeze_bof	2017-03-15	great	This module exploits a stack-based buffer overflow vulnerability in the web interface o Sync Breeze Enterprise v9.4.28, v10.0.28, v10.1.16, caused by improper bounds chec of the request in ... **Platforms**: win **CVEs**: CVE-2017-14980 **Refs**: source
Sysax Multi Server 5.64 Create Folder Buffer Overflow exploit/windows/http/sysax_create_folder	2012-07-29	normal	This module exploits a stack buffer overflo the create folder function in Sysax Multi Se 5.64. This issue was fixed in 5.66. In order trigger the vulnerability valid credentials wi ... **Platforms**: win **CVEs**: CVE-2012-6530 **Refs**: source, ref1, ref2
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability exploit/windows/http/tomcat_cgi_cmdlineargs	2019-04-10	excellent	This module exploits a vulnerability in Apac Tomcat's CGIServlet component. When the enableCmdLineArguments setting is set to a remote user can abuse this to execute sy commands, and gain ... **Platforms**: win **CVEs**: CVE-2019-0232 **Refs**: source, ref1, ref2
TrackerCam PHP Argument Buffer Overflow exploit/windows/http/trackercam_phparg_overflow	2005-02-18	average	This module exploits a simple stack buffer overflow in the TrackerCam web server. Al current versions of this software are vulner to a large number of security issues. This module abuses the ... **Platforms**: win **CVEs**: CVE-2005-0478 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Numara / BMC Track-It! FileStorageService Arbitrary File Upload exploit/windows/http/trackit_file_upload	2014-10-07	excellent	This module exploits an arbitrary file uploa vulnerability in Numara / BMC Track-It! v8 v11.X. The application exposes the FileStorageService .NET remoting service port 9010 (9004 for version ... **Platforms**: win **CVEs**: CVE-2014-4872 **Refs**: source, ref1
Trend Micro OfficeScan Remote Stack Buffer Overflow exploit/windows/http/trendmicro_officescan	2007-06-28	good	This module exploits a stack buffer overflo Trend Micro OfficeScan cgiChkMasterPwd (running with SYSTEM privileges). **Platforms**: win **CVEs**: CVE-2008-1365 **Refs**: source
Trend Micro OfficeScan Remote Code Execution exploit/windows/http/trendmicro_officescan_widget_exec	2017-10-07	excellent	This module exploits the authentication byp and command injection vulnerability togeth Unauthenticated users can execute a term command under the context of the web ser user. The ... **Platforms**: win **CVEs**: CVE-2017-11394 **Refs**: source, ref1, ref2
Ultra Mini HTTPD Stack Buffer Overflow exploit/windows/http/ultraminihttp_bof	2013-07-10	normal	This module exploits a stack based buffer overflow in Ultra Mini HTTPD 1.21, allowing remote attackers to execute arbitrary code long resource name in an HTTP request. T exploit has to deal ... **Platforms**: win **CVEs**: CVE-2013-5019 **Refs**: source
Umbraco CMS Remote Command Execution exploit/windows/http/umbraco_upload_aspx	2012-06-28	excellent	This module can be used to execute a pay on Umbraco CMS 4.7.0.378. The payload uploaded as an ASPX script by sending a specially crafted SOAP request to codeEditorSave.asmx, which permits ... **Platforms**: win **Refs**: source, ref1, ref2
VMware vCenter Chargeback Manager ImageUploadServlet Arbitrary File Upload exploit/windows/http/vmware_vcenter_chargeback_upload	2013-05-15	excellent	This module exploits a code execution flaw VMware vCenter Chargeback Manager, wh the ImageUploadServlet servlet allows unauthenticated file upload. The files are uploaded to the /cbmui/images/ ... **Platforms**: win **CVEs**: CVE-2013-3520 **Refs**: source
VX Search Enterprise GET Buffer Overflow exploit/windows/http/vxsrchs_bof	2017-03-15	great	This module exploits a stack-based buffer overflow vulnerability in the web interface o Search Enterprise v9.5.12, caused by impr bounds checking of the request path in HT GET requests sent ... **Platforms**: win **Refs**: source
Webster HTTP Server GET Buffer Overflow exploit/windows/http/webster_http	2002-12-02	average	This exploits a stack buffer overflow in the Webster HTTP server. The server and sou code was released within an article from th Microsoft Systems Journal in February 199 titled "Write a Simple ... **Platforms**: win **CVEs**: CVE-2002-2268 **Refs**: source, ref1, ref2
XAMPP WebDAV PHP Upload exploit/windows/http/xampp_webdav_upload_php	2012-01-14	excellent	This module exploits weak WebDAV passv on XAMPP servers. It uses supplied crede to upload a PHP payload and execute it. **Platforms**: php **Refs**: source

Metasploit Module	Date	Rank	Details
Xitami 2.5c2 Web Server If-Modified-Since Overflow exploit/windows/http/xitami_if_mod_since	2007-09-24	average	This module exploits a stack buffer overflo the iMatix Corporation Xitami Web Server. malicious user sends an If-Modified-Since header containing an overly long string, it r be possible ... **Platforms**: win **CVEs**: CVE-2007-5067 **Refs**: source
ZenTao Pro 8.8.2 Remote Code Execution exploit/windows/http/zentao_pro_rce	2020-06-20	excellent	This module exploits a command injection vulnerability in ZenTao Pro 8.8.2 and earlie versions in order to execute arbitrary comn with SYSTEM privileges. The module first attempts to ... **Platforms**: win **CVEs**: CVE-2020-7361 **Refs**: source
Novell ZENworks Asset Management Remote Execution exploit/windows/http/zenworks_assetmgmt_uploadservlet	2011-11-02	excellent	This module exploits a path traversal flaw i Novell ZENworks Asset Management 7.5. exploiting the CatchFileServlet, an attacke upload a malicious file outside of the MalibuUploadDirectory ... **Platforms**: java **CVEs**: CVE-2011-2653 **Refs**: source, ref1
Novell ZENworks Configuration Management Remote Execution exploit/windows/http/zenworks_uploadservlet	2010-03-30	excellent	This module exploits a code execution flaw Novell ZENworks Configuration Manageme 10.2.0. By exploiting the UploadServlet, an attacker can upload a malicious file outside the TEMP directory ... **Platforms**: java, linux, win **CVEs**: CVE-2010-5324 **Refs**: source, ref1, ref2
IBM Websphere Application Server Network Deployment Untrusted Data Deserialization Remote Code Execution exploit/windows/ibm/ibm_was_dmgr_java_deserialization_rce	2019-05-15	excellent	This module exploits untrusted serialized d processed by the WAS DMGR Server and NOTE: There is a required 2 minute timeou between attempts as the neighbor being ac must be reset. **Platforms**: win **CVEs**: CVE-2019-4279 **Refs**: source, ref1
Microsoft IIS WebDav ScStoragePathFromUrl Overflow exploit/windows/iis/iis_webdav_scstoragepathfromurl	2017-03-26	manual	Buffer overflow in the ScStoragePathFrom function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary ... **Platforms**: win **CVEs**: CVE-2017-7269 **Refs**: source, ref1, ref2
Microsoft IIS WebDAV Write Access Code Execution exploit/windows/iis/iis_webdav_upload_asp	2004-12-31	excellent	This module can be used to execute a pay on IIS servers that have world-writeable directories. The payload is uploaded as an script via a WebDAV PUT request. The tar IIS machine must meet ... **Platforms**: win **Refs**: source
MS01-023 Microsoft IIS 5.0 Printer Host Header Overflow exploit/windows/iis/ms01_023_printer	2001-05-01	good	This exploits a buffer overflow in the reque processor of the Internet Printing Protocol module in IIS. This module works against Windows 2000 service pack 0 and 1. If the service stops ... **Platforms**: win **CVEs**: CVE-2001-0241 **Refs**: source, ref1
MS01-026 Microsoft IIS/PWS CGI Filename Double Decode Command Execution exploit/windows/iis/ms01_026_dbldecode	2001-05-15	excellent	This module will execute an arbitrary paylo a Microsoft IIS installation that is vulnerabl the CGI double-decode vulnerability of 200 NOTE: This module will leave a metasploit payload in ... **Platforms**: win **CVEs**: CVE-2001-0333 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
MS01-033 Microsoft IIS 5.0 IDQ Path Overflow exploit/windows/iis/ms01_033_idq	2001-06-18	good	This module exploits a stack buffer overflo the IDQ ISAPI handler for Microsoft Index Server. **Platforms**: win **CVEs**: CVE-2001-0500 **Refs**: source
MS02-018 Microsoft IIS 4.0 .HTR Path Overflow exploit/windows/iis/ms02_018_htr	2002-04-10	good	This exploits a buffer overflow in the ISAPI ISM.DLL used to process HTR scripting in 4.0. This module works against Windows N Service Packs 3, 4, and 5. The server will continue to process ... **Platforms**: win **CVEs**: CVE-1999-0874 **Refs**: source, ref1
MS02-065 Microsoft IIS MDAC msadcs.dll RDS DataStub Content-Type Overflow exploit/windows/iis/ms02_065_msadc	2002-11-20	normal	This module can be used to execute arbitra code on IIS servers that expose the /msadc/msadcs.dll Microsoft Data Access Components (MDAC) Remote Data Servic (RDS) DataFactory service. The service ... **Platforms**: win **CVEs**: CVE-2002-1142 **Refs**: source, ref1
MS03-007 Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow exploit/windows/iis/ms03_007_ntdll_webdav	2003-05-30	great	This exploits a buffer overflow in NTDLL.dl Windows 2000 through the SEARCH Webl method in IIS. This particular module only v against Windows 2000. It should have a reasonable chance of ... **Platforms**: win **CVEs**: CVE-2003-0109 **Refs**: source
MS99-025 Microsoft IIS MDAC msadcs.dll RDS Arbitrary Remote Command Execution exploit/windows/iis/msadc	1998-07-17	excellent	This module can be used to execute arbitra commands on IIS servers that expose the /msadc/msadcs.dll Microsoft Data Access Components (MDAC) Remote Data Servic (RDS) DataFactory service using ... **Platforms**: win **CVEs**: CVE-1999-1011 **Refs**: source
Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow exploit/windows/imap/eudora_list	2005-12-20	great	This module exploits a stack buffer overflo the Qualcomm WorldMail IMAP Server ver 3.0 (builds 6.1.19.0 through 6.1.22.0). Vers 6.1.22.1 fixes this particular vulnerability. N The ... **Platforms**: win **CVEs**: CVE-2005-4267 **Refs**: source
IMail IMAP4D Delete Overflow exploit/windows/imap/imail_delete	2004-11-12	average	This module exploits a buffer overflow in th 'DELETE' command of the IMail IMAP4D service. This vulnerability can only be explo with a valid username and password. This was patched in ... **Platforms**: win **CVEs**: CVE-2004-1520 **Refs**: source
Ipswitch IMail IMAP SEARCH Buffer Overflow exploit/windows/imap/ipswitch_search	2007-07-18	average	This module exploits a stack buffer overflo Ipswitch IMail Server 2006.1 IMAP SEARC verb. By sending an overly long string, an attacker can overwrite the buffer and contr program execution. In ... **Platforms**: win **CVEs**: CVE-2007-3925 **Refs**: source
MailEnable IMAPD (2.34/2.35) Login Request Buffer Overflow exploit/windows/imap/mailenable_login	2006-12-11	great	MailEnable's IMAP server contains a buffe overflow vulnerability in the Login comman **Platforms**: win **CVEs**: CVE-2006-6423 **Refs**: source

Metasploit Module	Date	Rank	Details
MailEnable IMAPD (1.54) STATUS Request Buffer Overflow exploit/windows/imap/mailenable_status	2005-07-13	great	MailEnable's IMAP server contains a buffe overflow vulnerability in the STATUS comm With proper credentials, this could allow fo execution of arbitrary code. **Platforms**: win **CVEs**: CVE-2005-2278 **Refs**: source, ref1
MailEnable IMAPD W3C Logging Buffer Overflow exploit/windows/imap/mailenable_w3c_select	2005-10-03	great	This module exploits a buffer overflow in th W3C logging functionality of the MailEnabl IMAPD service. Logging is not enabled by default and this exploit requires a valid username and password to ... **Platforms**: win **CVEs**: CVE-2005-3155 **Refs**: source
Mdaemon 8.0.3 IMAPD CRAM-MD5 Authentication Overflow exploit/windows/imap/mdaemon_cram_md5	2004-11-12	great	This module exploits a buffer overflow in th CRAM-MD5 authentication of the MDaemc IMAP service. This vulnerability was discov by Muts. **Platforms**: win **CVEs**: CVE-2004-1520 **Refs**: source
MDaemon 9.6.4 IMAPD FETCH Buffer Overflow exploit/windows/imap/mdaemon_fetch	2008-03-13	great	This module exploits a stack buffer overflo the Alt-N MDaemon IMAP Server version 9 by sending an overly long FETCH BODY command. Valid IMAP account credentials required. Credit to Matteo ... **Platforms**: win **CVEs**: CVE-2008-1358 **Refs**: source
Mercury/32 4.01 IMAP LOGIN SEH Buffer Overflow exploit/windows/imap/mercury_login	2007-03-06	normal	This module exploits a stack buffer overflo Mercury/32 <= 4.01b IMAPD LOGIN verb. sending a specially crafted login command buffer is corrupted, and code execution is possible. This ... **Platforms**: win **CVEs**: CVE-2007-1373 **Refs**: source
Mercury/32 v4.01a IMAP RENAME Buffer Overflow exploit/windows/imap/mercury_rename	2004-11-29	average	This module exploits a stack buffer overflo vulnerability in the Mercury/32 v.4.01a IMA service. **Platforms**: win **CVEs**: CVE-2004-1211 **Refs**: source, ref1
Mercur v5.0 IMAP SP3 SELECT Buffer Overflow exploit/windows/imap/mercur_imap_select_overflow	2006-03-17	average	Mercur v5.0 IMAP server is prone to a rem exploitable stack-based buffer overflow vulnerability. This issue is due to a failure c application to properly bounds check user-supplied data ... **Platforms**: win **CVEs**: CVE-2006-1255 **Refs**: source
Mercur Messaging 2005 IMAP Login Buffer Overflow exploit/windows/imap/mercur_login	2006-03-17	average	This module exploits a stack buffer overflo Atrium Mercur IMAP 5.0 SP3. Since the ro for shellcode is small, using the reverse or payloads yields the best results. **Platforms**: win **CVEs**: CVE-2006-1255 **Refs**: source, ref1
Novell NetMail IMAP APPEND Buffer Overflow exploit/windows/imap/novell_netmail_append	2006-12-23	average	This module exploits a stack buffer overflo Novell's Netmail 3.52 IMAP APPEND verb sending an overly long string, an attacker c overwrite the buffer and control program execution. **Platforms**: win **CVEs**: CVE-2006-6425 **Refs**: source

Metasploit Module	Date	Rank	Details
Novell NetMail IMAP AUTHENTICATE Buffer Overflow exploit/windows/imap/novell_netmail_auth	2007-01-07	average	This module exploits a stack buffer overflo Novell's NetMail 3.52 IMAP AUTHENTICA GSSAPI command. By sending an overly l string, an attacker can overwrite the buffer control program ... **Platforms**: win **Refs**: source
Novell NetMail IMAP STATUS Buffer Overflow exploit/windows/imap/novell_netmail_status	2005-11-18	average	This module exploits a stack buffer overflo Novell's NetMail 3.52 IMAP STATUS verb. sending an overly long string, an attacker c overwrite the buffer and control program execution. **Platforms**: win **CVEs**: CVE-2005-3314 **Refs**: source
Novell NetMail IMAP SUBSCRIBE Buffer Overflow exploit/windows/imap/novell_netmail_subscribe	2006-12-23	average	This module exploits a stack buffer overflo Novell's NetMail 3.52 IMAP SUBSCRIBE v By sending an overly long string, an attack can overwrite the buffer and control progra execution. **Platforms**: win **CVEs**: CVE-2006-6761 **Refs**: source, ref1
MS00-094 Microsoft IIS Phone Book Service Overflow exploit/windows/isapi/ms00_094_pbserver	2000-12-04	good	This is an exploit for the Phone Book Servi /pbserver/pbserver.dll described in MS00-0 By sending an overly long URL argument f phone book updates, it is possible to overv the stack. This ... **Platforms**: win **CVEs**: CVE-2000-1089 **Refs**: source
MS03-022 Microsoft IIS ISAPI nsiislog.dll ISAPI POST Overflow exploit/windows/isapi/ms03_022_nsiislog_post	2003-06-25	good	This exploits a buffer overflow found in the nsiislog.dll ISAPI filter that comes with Win Media Server. This module will also work against the 'patched' MS03-019 version. TI vulnerability was ... **Platforms**: win **CVEs**: CVE-2003-0349 **Refs**: source, ref1
MS03-051 Microsoft IIS ISAPI FrontPage fp30reg.dll Chunked Overflow exploit/windows/isapi/ms03_051_fp30reg_chunked	2003-11-11	good	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 Windows 2000 between SP0 ... **Platforms**: win **CVEs**: CVE-2003-0822 **Refs**: source
Microsoft IIS ISAPI RSA WebAgent Redirect Overflow exploit/windows/isapi/rsa_webagent_redirect	2005-10-21	good	This module exploits a stack buffer overflo the SecurID Web Agent for IIS. This ISAPI runs in-process with inetinfo.exe, any atten exploit this flaw will result in the terminatior ... **Platforms**: win **CVEs**: CVE-2005-4734 **Refs**: source
Microsoft IIS ISAPI w3who.dll Query String Overflow exploit/windows/isapi/w3who_query	2004-12-06	good	This module exploits a stack buffer overflo the w3who.dll ISAPI application. This vulnerability was discovered Nicolas Grego and this code has been successfully testec against Windows 2000 and ... **Platforms**: win **CVEs**: CVE-2004-1134 **Refs**: source, ref1
IMail LDAP Service Buffer Overflow exploit/windows/ldap/imail_thc	2004-02-17	average	This exploits a buffer overflow in the LDAP service that is part of the IMail product. Thi module was tested against version 7.10 an 8.5, both running on Windows 2000. **Platforms**: win **CVEs**: CVE-2004-0297 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Network Associates PGP KeyServer 7 LDAP Buffer Overflow exploit/windows/ldap/pgp_keyserver7	2001-07-16	good	This module exploits a stack buffer overflo the LDAP service that is part of the NAI PG Enterprise product suite. This module was tested against PGP KeyServer v7.0. Due t space restrictions, ... **Platforms**: win **CVEs**: CVE-2001-1320 **Refs**: source, ref1
Computer Associates License Client GETCONFIG Overflow exploit/windows/license/calicclnt_getconfig	2005-03-02	average	This module exploits a vulnerability in the C License Client service. This exploit will onl work if your IP address can be resolved fro the target system point of view. This can be accomplished on ... **Platforms**: win **CVEs**: CVE-2005-0581 **Refs**: source, ref1
Computer Associates License Server GETCONFIG Overflow exploit/windows/license/calicserv_getconfig	2005-03-02	normal	This module exploits an vulnerability in the License Server network service. By sendin excessively long GETCONFIG packet the s may be overwritten. **Platforms**: win **CVEs**: CVE-2005-0581 **Refs**: source, ref1
FlexNet License Server Manager lmgrd Buffer Overflow exploit/windows/license/flexnet_lmgrd_bof	2012-03-23	normal	This module exploits a vulnerability in the FlexNet License Server Manager. The vulnerability is due to the insecure usage o memcpy in the lmgrd service when handlin network packets, which results ... **Platforms**: win **Refs**: source, ref1, ref2
SentinelLM UDP Buffer Overflow exploit/windows/license/sentinel_lm7_udp	2005-03-07	average	This module exploits a simple stack buffer overflow in the Sentinel License Manager. SentinelLM service is installed with a wide selection of products and seems particular popular with academic ... **Platforms**: win **CVEs**: CVE-2005-0353 **Refs**: source
IBM Lotus Domino Web Server Accept-Language Stack Buffer Overflow exploit/windows/lotus/domino_http_accept_language	2008-05-20	average	This module exploits a stack buffer overflo IBM Lotus Domino Web Server prior to ver 7.0.3FP1 and 8.0.1. This flaw is triggered b any HTTP request with an Accept-Languag header greater than ... **Platforms**: win **CVEs**: CVE-2008-2240 **Refs**: source, ref1
IBM Lotus Domino iCalendar MAILTO Buffer Overflow exploit/windows/lotus/domino_icalendar_organizer	2010-09-14	normal	This module exploits a vulnerability found i Lotus Domino iCalendar. By sending a long string of data as the "ORGANIZER,mailto" header, process "nRouter.exe" crashes due Cstrcpy() routine ... **Platforms**: win **CVEs**: CVE-2010-3407 **Refs**: source, ref1, ref2
IBM Lotus Domino Sametime STMux.exe Stack Buffer Overflow exploit/windows/lotus/domino_sametime_stmux	2008-05-21	average	This module exploits a stack buffer overflo Lotus Domino's Sametime Server. By send an overly long POST request to the Multipl STMux.exe service we are able to overwrit SEH. Based on the ... **Platforms**: win **CVEs**: CVE-2008-2499 **Refs**: source
Lotus Notes 8.0.x - 8.5.2 FP2 - Autonomy Keyview (.lzh Attachment) exploit/windows/lotus/lotusnotes_lzh	2011-05-24	normal	This module exploits a stack buffer overflo Lotus Notes 8.5.2 when parsing a malform specially crafted LZH file. This vulnerability discovered binaryhouse.net. **Platforms**: win **CVEs**: CVE-2011-1213 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Hummingbird Connectivity 10 SP5 LPD Buffer Overflow exploit/windows/lpd/hummingbird_exceed	2005-05-27	average	This module exploits a stack buffer overflo Hummingbird Connectivity 10 LPD Daemo This module has only been tested against Hummingbird Exceed v10 with SP5. **Platforms**: win **CVEs**: CVE-2005-1815 **Refs**: source
NIPrint LPD Request Overflow exploit/windows/lpd/niprint	2003-11-05	good	This module exploits a stack buffer overflo the Network Instrument NIPrint LPD servic Inspired by Immunity's VisualSploit :-). **Platforms**: win **CVEs**: CVE-2003-1141 **Refs**: source, ref1
SAP SAPLPD 6.28 Buffer Overflow exploit/windows/lpd/saplpd	2008-02-04	good	This module exploits a stack buffer overflo SAPlpd 6.28 (SAP Release 6.40) . By send an overly long argument, an attacker may l able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2008-0621 **Refs**: source
WinComLPD Buffer Overflow exploit/windows/lpd/wincomlpd_admin	2008-02-04	good	This module exploits a stack buffer overflo WinComLPD <= 3.0.2. By sending an over long authentication packet to the remote administration service, an attacker may be to execute arbitrary ... **Platforms**: win **CVEs**: CVE-2008-5159 **Refs**: source
Achat Unicode SEH Buffer Overflow exploit/windows/misc/achat_bof	2014-12-18	normal	This module exploits a Unicode SEH buffe overflow in Achat. By sending a crafted message to the default port 9256/UDP, it's possible to overwrite the SEH handler. Eve when the exploit is reliable, ... **Platforms**: win **Refs**: source
ActFax 5.01 RAW Server Buffer Overflow exploit/windows/misc/actfax_raw_server_bof	2013-02-05	normal	This module exploits a vulnerability in ActF Server 5.01 RAW server. The RAW Server be used to transfer fax messages without a underlying protocols. To note significant fie the fax ... **Platforms**: win **Refs**: source, ref1
AgentX++ Master AgentX::receive_agentx Stack Buffer Overflow exploit/windows/misc/agentxpp_receive_agentx	2010-04-16	good	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 potentially with SYSTEM ... **Platforms**: win **CVEs**: CVE-2010-1318 **Refs**: source, ref1
Ahsay Backup v7.x-v8.1.1.50 (authenticated) file upload exploit/windows/misc/ahsay_backup_fileupload	2019-06-01	excellent	This module exploits an authenticated inse file upload and code execution flaw in Ahsa Backup v7.x - v8.1.1.50. To succesfully exe the upload credentials are needed, default Ahsay Backup ... **Platforms**: linux, win **CVEs**: CVE-2019-10267 **Refs**: source, ref1, ref2
AIS logistics ESEL-Server Unauth SQL Injection RCE exploit/windows/misc/ais_esel_server_rce	2019-03-27	excellent	This module will execute an arbitrary paylo an "ESEL" server used by the AIS logistic software. The server typically listens on po 5099 without TLS. There could also be ser listening on ... **Platforms**: win **CVEs**: CVE-2019-10123 **Refs**: source

Metasploit Module	Date	Rank	Details
ALLMediaServer 0.8 Buffer Overflow exploit/windows/misc/allmediaserver_bof	2012-07-04	normal	This module exploits a stack buffer overflo ALLMediaServer 0.8. The vulnerability is caused due to a boundary error within the handling of HTTP request. While the explo supports DEP bypass via ... **Platforms**: win **CVEs**: CVE-2017-17932 **Refs**: source
Symantec Altiris DS SQL Injection exploit/windows/misc/altiris_ds_sqli	2008-05-15	normal	This module exploits a SQL injection flaw i Symantec Altiris Deployment Solution 6.8 t 6.9.164. The vulnerability exists on axengine.exe which fails to adequately sar numeric input fields in ... **Platforms**: win **CVEs**: CVE-2008-2286 **Refs**: source, ref1
Apple QuickTime 7.3 RTSP Response Header Buffer Overflow exploit/windows/misc/apple_quicktime_rtsp_response	2007-11-23	normal	This module exploits a stack buffer overflo Apple QuickTime 7.3. By sending an overly RTSP response to a client, an attacker ma able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2007-6166 **Refs**: source
Asus Dpcproxy Buffer Overflow exploit/windows/misc/asus_dpcproxy_overflow	2008-03-21	average	This module exploits a stack buffer overflo Asus Dpcroxy version 2.0.0.19. It should b vulnerable until version 2.0.0.24. Credit to Auriemma. **Platforms**: win **CVEs**: CVE-2008-1491 **Refs**: source
Avaya WinPMD UniteHostRouter Buffer Overflow exploit/windows/misc/avaya_winpmd_unihostrouter	2011-05-23	normal	This module exploits a stack buffer overflo Avaya WinPMD. The vulnerability exists in UniteHostRouter service, due to the insecu usage of memcpy when parsing specially crafted "To:" ... **Platforms**: win **Refs**: source, ref1, ref2
Avid Media Composer 5.5 - Avid Phonetic Indexer Buffer Overflow exploit/windows/misc/avidphoneticindexer	2011-11-29	normal	This module exploits a stack buffer overflo process AvidPhoneticIndexer.exe (port 465 which comes as part of the Avid Media Composer 5.5 Editing Suite. This daemon sometimes starts on a ... **Platforms**: win **CVEs**: CVE-2011-5003 **Refs**: source, ref1
BakBone NetVault Remote Heap Overflow exploit/windows/misc/bakbone_netvault_heap	2005-04-01	average	This module exploits a heap overflow in the BakBone NetVault Process Manager servic This code is a direct port of the netvault.c c written by nolimit and BuzzDee. **Platforms**: win **CVEs**: CVE-2005-1009 **Refs**: source
Blue Coat Authentication and Authorization Agent (BCAAA) 5 Buffer Overflow exploit/windows/misc/bcaaa_bof	2011-04-04	good	This module exploits a stack buffer overflo process bcaaa-130.exe (port 16102 which comes as part of the Blue Coat Authentica proxy. Please note that by default, this exp will attempt up ... **Platforms**: win **CVEs**: CVE-2011-5124 **Refs**: source, ref1, ref2
BigAnt Server 2.2 Buffer Overflow exploit/windows/misc/bigant_server	2008-04-15	average	This module exploits a stack buffer overflo BigAnt Server 2.2. By sending a specially crafted packet, an attacker may be able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2008-1914 **Refs**: source

Metasploit Module	Date	Rank	Details
BigAnt Server 2.50 SP1 Buffer Overflow exploit/windows/misc/bigant_server_250	2008-04-15	great	This exploits a stack buffer overflow in the BigAnt Messaging Service, part of the BigA Server product suite. This module was test successfully against version 2.50 SP1. **Platforms**: win **CVEs**: CVE-2008-1914 **Refs**: source
BigAnt Server 2 SCH And DUPF Buffer Overflow exploit/windows/misc/bigant_server_sch_dupf_bof	2013-01-09	normal	This exploits a stack buffer overflow in BigA Server 2.97 SP7. The vulnerability is due t dangerous usage of strcpy while handling errors. This module uses a combination of and DUPF ... **Platforms**: win **CVEs**: CVE-2012-6275 **Refs**: source
BigAnt Server 2.52 USV Buffer Overflow exploit/windows/misc/bigant_server_usv	2009-12-29	great	This exploits a stack buffer overflow in the BigAnt Messaging Service, part of the BigA Server product suite. This module was test successfully against version 2.52. NOTE: T AntServer service ... **Platforms**: win **CVEs**: CVE-2009-4660 **Refs**: source
Bomberclone 0.11.6 Buffer Overflow exploit/windows/misc/bomberclone_overflow	2006-02-16	average	This module exploits a stack buffer overflo Bomberclone 0.11.6 for Windows. The retu address is overwritten with lstrcpyA memor address, the second and third value are the destination buffer, ... **Platforms**: win **CVEs**: CVE-2006-0460 **Refs**: source
Bopup Communications Server Buffer Overflow exploit/windows/misc/bopup_comm	2009-06-18	good	This module exploits a stack buffer overflo Bopup Communications Server 3.2.26.546 sending a specially crafted packet, an attac may be able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2009-2227 **Refs**: source, ref1
Borland Interbase Create-Request Buffer Overflow exploit/windows/misc/borland_interbase	2007-07-24	average	This module exploits a stack buffer overflo Borland Interbase 2007. By sending a spec crafted create-request packet, a remote att may be able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2007-3566 **Refs**: source, ref1
Borland CaliberRM StarTeam Multicast Service Buffer Overflow exploit/windows/misc/borland_starteam	2008-04-02	average	This module exploits a stack buffer overflo Borland CaliberRM 2006. By sending a spe crafted GET request to the STMulticastSer an attacker may be able to execute arbitrar code. **Platforms**: win **CVEs**: CVE-2008-0311 **Refs**: source
Citrix Provisioning Services 5.6 streamprocess.exe Buffer Overflow exploit/windows/misc/citrix_streamprocess	2011-01-20	good	This module exploits a stack buffer overflo Citrix Provisioning Services 5.6. By sendin specially crafted packet to the Provisioning Services server, a fixed length buffer on the stack can be ... **Platforms**: win **Refs**: source, ref1, ref2
Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020000 Buffer Overflow exploit/windows/misc/citrix_streamprocess_data_msg	2011-11-04	normal	This module exploits a remote buffer overfl the Citrix Provisioning Services 5.6 SP1 (w Hotfix CPVS56SP1E043) by sending a malformed packet to the 6905/UDP port. T module has been ... **Platforms**: win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020004 Buffer Overflow exploit/windows/misc/citrix_streamprocess_get_boot_record_request	2011-11-04	normal	This module exploits a remote buffer overfl the Citrix Provisioning Services 5.6 SP1 (w Hotfix CPVS56SP1E043) by sending a malformed packet with the opcode 0x4002 ... **Platforms**: win **Refs**: source, ref1
Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020002 Buffer Overflow exploit/windows/misc/citrix_streamprocess_get_footer	2011-11-04	normal	This module exploits a remote buffer overfl the Citrix Provisioning Services 5.6 SP1 (w Hotfix CPVS56SP1E043) by sending a malformed packet with the opcode 0x4002 (GetFooterRequest) to ... **Platforms**: win **Refs**: source, ref1
Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020006 Buffer Overflow exploit/windows/misc/citrix_streamprocess_get_objects	2011-11-04	normal	This module exploits a remote buffer overfl the Citrix Provisioning Services 5.6 SP1 (w Hotfix CPVS56SP1E043) by sending a malformed packet with the opcode 0x4002 (GetObjetsRequest) to ... **Platforms**: win **Refs**: source, ref1
CloudMe Sync v1.10.9 exploit/windows/misc/cloudme_sync	2018-01-17	great	This module exploits a stack-based buffer overflow vulnerability in CloudMe Sync v1. client application. This module has been te successfully on Windows 7 SP1 x86. **Platforms**: win **CVEs**: CVE-2018-6892 **Refs**: source
Commvault Communications Service (cvd) Command Injection exploit/windows/misc/commvault_cmd_exec	2017-12-12	good	This module exploits a command injection vulnerability discovered in Commvault Serv v11 SP5 and earlier versions (tested in v11 and v10). The vulnerability exists in the cvd service and ... **Platforms**: win **CVEs**: CVE-2017-18044 **Refs**: source, ref1
Anviz CrossChex Buffer Overflow exploit/windows/misc/crosschex_device_bof	2019-11-28	normal	Waits for broadcasts from Ainz CrossChex looking for new devices, and returns a cust broadcast, triggering a stack buffer overflo **Platforms**: win **CVEs**: CVE-2019-12518 **Refs**: source, ref1
Disk Savvy Enterprise v10.4.18 exploit/windows/misc/disk_savvy_adm	2017-01-31	great	This module exploits a stack-based buffer overflow vulnerability in Disk Savvy Enterp v10.4.18, caused by improper bounds chec of the request sent to the built-in server. Th module has been ... **Platforms**: win **CVEs**: CVE-2018-6481 **Refs**: source
eIQNetworks ESA License Manager LICMGR_ADDLICENSE Overflow exploit/windows/misc/eiqnetworks_esa	2006-07-24	average	This module exploits a stack buffer overflo eIQnetworks Enterprise Security Analyzer. During the processing of long arguments to LICMGR_ADDLICENSE command, a stac based buffer overflow ... **Platforms**: win **CVEs**: CVE-2006-3838 **Refs**: source
eIQNetworks ESA Topology DELETEDEVICE Overflow exploit/windows/misc/eiqnetworks_esa_topology	2006-07-25	average	This module exploits a stack buffer overflo eIQnetworks Enterprise Security Analyzer. During the processing of long arguments to DELETEDEVICE command in the Topolog server, a stack-based ... **Platforms**: win **CVEs**: CVE-2006-3838 **Refs**: source

Metasploit Module	Date	Rank	Details
Enterasys NetSight nssyslogd.exe Buffer Overflow exploit/windows/misc/enterasys_netsight_syslog_bof	2011-12-19	normal	This module exploits a stack buffer overflo Enterasys NetSight. The vulnerability exist the Syslog service (nssylogd.exe) when pa a specially crafted PRIO from a syslog message. The ... **Platforms**: win **CVEs**: CVE-2011-5227 **Refs**: source
Eureka Email 2.2q ERR Remote Buffer Overflow exploit/windows/misc/eureka_mail_err	2009-10-22	normal	This module exploits a buffer overflow in th Eureka Email 2.2q client that is triggered through an excessively long ERR message NOTE: this exploit isn't very reliable. Unfortunately reaching the ... **Platforms**: win **CVEs**: CVE-2009-3837 **Refs**: source
Firebird Relational Database CNCT Group Number Buffer Overflow exploit/windows/misc/fb_cnct_group	2013-01-31	normal	This module exploits a vulnerability in Fireb SQL Server. A specially crafted packet can sent which will overwrite a pointer allowing attacker to control where data is read from Shortly, ... **Platforms**: win **CVEs**: CVE-2013-2492 **Refs**: source
Firebird Relational Database isc_attach_database() Buffer Overflow exploit/windows/misc/fb_isc_attach_database	2007-10-03	average	This module exploits a stack buffer overflo Borland InterBase by sending a specially c create request. **Platforms**: win **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Firebird Relational Database isc_create_database() Buffer Overflow exploit/windows/misc/fb_isc_create_database	2007-10-03	average	This module exploits a stack buffer overflo Borland InterBase by sending a specially c create request. **Platforms**: win **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Firebird Relational Database SVC_attach() Buffer Overflow exploit/windows/misc/fb_svc_attach	2007-10-03	average	This module exploits a stack buffer overflo Borland InterBase by sending a specially c service attach request. **Platforms**: win **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Gh0st Client buffer Overflow exploit/windows/misc/gh0st	2017-07-27	normal	This module exploits a Memory buffer over in the Gh0st client (C2 server). **Platforms**: win **Refs**: source
GIMP script-fu Server Buffer Overflow exploit/windows/misc/gimp_script_fu	2012-05-18	normal	This module exploits a buffer overflow in th script-fu server component on GIMP <= 2.6 By sending a specially crafted packet, an attacker may be able to achieve remote co execution under the ... **Platforms**: win **CVEs**: CVE-2012-2763 **Refs**: source, ref1
HP Data Protector 8.10 Remote Command Execution exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	This module exploits a remote command execution on HP Data Protector 8.10. Arbit commands can be executed by sending cr requests with opcode 28 to the OmniInet s listening on the ... **Platforms**: win **CVEs**: CVE-2014-2623 **Refs**: source, ref1
HP Data Protector Cell Request Service Buffer Overflow exploit/windows/misc/hp_dataprotector_crs	2013-06-03	normal	This module exploits a stack-based buffer overflow in the Hewlett-Packard Data Prote product. The vulnerability, due to the insec usage of _swprintf, exists at the Cell Requ Service ... **Platforms**: win **CVEs**: CVE-2013-2333 **Refs**: source

Metasploit Module	Date	Rank	Details
HP Data Protector DtbClsLogin Buffer Overflow exploit/windows/misc/hp_dataprotector_dtbclslogin	2010-09-09	normal	This module exploits a stack buffer overflo 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 ... **Platforms**: win **CVEs**: CVE-2010-3007 **Refs**: source, ref1
HP Data Protector Encrypted Communication Remote Command Execution exploit/windows/misc/hp_dataprotector_encrypted_comms	2016-04-18	normal	This module exploits a well known remote execution exploit after establishing encrypt control communications with a Data Protec agent. This allows exploitation of Data Prot agents that ... **Platforms**: win **CVEs**: CVE-2016-2004 **Refs**: source, ref1
HP Data Protector 6.10/6.11/6.20 Install Service exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	This module exploits HP Data Protector OmniInet process on Windows only. This e invokes the install service function which a an attacker to create a custom payload in t format of an ... **Platforms**: win **CVEs**: CVE-2011-0922 **Refs**: source, ref1
HP Data Protector Create New Folder Buffer Overflow exploit/windows/misc/hp_dataprotector_new_folder	2012-03-12	normal	This module exploits a stack buffer overflo HP Data Protector 5. The overflow occurs creation of new folders, where the name of folder is handled in a insecure way by the dpwindtb.dll ... **Platforms**: win **CVEs**: CVE-2012-0124 **Refs**: source, ref1
HP Data Protector Backup Client Service Directory Traversal exploit/windows/misc/hp_dataprotector_traversal	2014-01-02	great	This module exploits a directory traversal vulnerability in the Hewlett-Packard Data Protector product. The vulnerability exists i Backup Client Service (OmniInet.exe) and triggered when ... **Platforms**: win **CVEs**: CVE-2013-6194 **Refs**: source, ref1
HPE iMC dbman RestartDB Unauthenticated RCE exploit/windows/misc/hp_imc_dbman_restartdb_unauth_rce	2017-05-15	excellent	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 ... **Platforms**: win **CVEs**: CVE-2017-5816 **Refs**: source, ref1
HPE iMC dbman RestoreDBase Unauthenticated RCE exploit/windows/misc/hp_imc_dbman_restoredbase_unauth_rce	2017-05-15	excellent	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 ... **Platforms**: win **CVEs**: CVE-2017-5817 **Refs**: source, ref1
HP Intelligent Management Center UAM Buffer Overflow exploit/windows/misc/hp_imc_uam	2012-08-29	normal	This module exploits a remote buffer overfl HP Intelligent Management Center UAM. T vulnerability exists in the uam.exe compon when using sprint in a insecure way for log purposes. The ... **Platforms**: win **CVEs**: CVE-2012-3274 **Refs**: source, ref1
HP LoadRunner magentproc.exe Overflow exploit/windows/misc/hp_loadrunner_magentproc	2013-07-27	normal	This module exploits a stack buffer overflo HP LoadRunner before 11.52. The vulnera exists on the LoadRunner Agent Process magentproc.exe. By sending a specially cr packet, an attacker ... **Platforms**: win **CVEs**: CVE-2013-4800 **Refs**: source

Metasploit Module	Date	Rank	Details
HP Mercury LoadRunner Agent magentproc.exe Remote Command Execution exploit/windows/misc/hp_loadrunner_magentproc_cmdexec	2010-05-06	excellent	This module exploits a remote command execution vulnerablity in HP LoadRunner b 9.50 and also HP Performance Center befc 9.50. HP LoadRunner 12.53 and other vers are also most likely ... **Platforms**: win **CVEs**: CVE-2010-1549 **Refs**: source, ref1
HP Diagnostics Server magentservice.exe Overflow exploit/windows/misc/hp_magentservice	2012-01-12	average	This module exploits a stack buffer overflo HP Diagnostics Server magentservice.exe service. By sending a specially crafted pac an attacker may be able to execute arbitrai code. Originally ... **Platforms**: win **CVEs**: CVE-2011-4789 **Refs**: source
HP Omnilnet.exe MSG_PROTOCOL Buffer Overflow exploit/windows/misc/hp_omniinet_1	2009-12-17	great	This module exploits a stack-based buffer overflow in the Hewlett-Packard OmniInet I Service. By sending a specially crafted MSG_PROTOCOL (0x010b) packet, a rem attacker may be able to execute ... **Platforms**: win **CVEs**: CVE-2007-2280 **Refs**: source
HP Omnilnet.exe MSG_PROTOCOL Buffer Overflow exploit/windows/misc/hp_omniinet_2	2009-12-17	great	This module exploits a stack-based buffer overflow in the Hewlett-Packard OmniInet I Service. By sending a specially crafted MSG_PROTOCOL (0x010b) packet, a rem attacker may be able to execute ... **Platforms**: win **CVEs**: CVE-2009-3844 **Refs**: source
HP Omnilnet.exe Opcode 27 Buffer Overflow exploit/windows/misc/hp_omniinet_3	2011-06-29	great	This module exploits a buffer overflow in th Hewlett-Packard OmniInet NT Service. By sending a specially crafted opcode 27 pacl remote attacker may be able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2011-1865 **Refs**: source, ref1
HP Omnilnet.exe Opcode 20 Buffer Overflow exploit/windows/misc/hp_omniinet_4	2011-06-29	good	This module exploits a vulnerability found i Data Protector's OmniInet process. By supplying a long string of data as the file pa with opcode '20 a buffer overflow can occu when this data is ... **Platforms**: win **CVEs**: CVE-2011-1865 **Refs**: source, ref1, ref2
HP Operations Agent Opcode coda.exe 0x34 Buffer Overflow exploit/windows/misc/hp_operations_agent_coda_34	2012-07-09	normal	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 ... **Platforms**: win **CVEs**: CVE-2012-2019 **Refs**: source
HP Operations Agent Opcode coda.exe 0x8c Buffer Overflow exploit/windows/misc/hp_operations_agent_coda_8c	2012-07-09	normal	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 ... **Platforms**: win **CVEs**: CVE-2012-2020 **Refs**: source
BigAnt Server DUPF Command Arbitrary File Upload exploit/windows/misc/bigant_server_dupf_upload	2013-01-09	excellent	This exploits an arbitrary file upload vulner in BigAnt Server 2.97 SP7. A lack of authentication allows to make unauthentica file uploads through a DUPF command. Additionally the filename ... **Platforms**: win **CVEs**: CVE-2012-6274 **Refs**: source

Metasploit Module	Date	Rank	Details
DoubleTake/HP StorageWorks Storage Mirroring Service Authentication Overflow exploit/windows/misc/doubletake	2008-06-04	average	This module exploits a stack buffer overflo the authentication mechanism of NSI Doubletake which is also rebranded as HP Storage Works. This vulnerability was foun Titon of Bastard Labs. **Platforms**: win **CVEs**: CVE-2008-1661 **Refs**: source
HP Data Protector Backup Client Service Remote Code Execution exploit/windows/misc/hp_dataprotector_exec_bar	2014-01-02	excellent	This module abuses the Backup Client Ser (OmniInet.exe) to achieve remote code execution. The vulnerability exists in the EXEC_BAR operation, which allows to exe arbitrary processes. This ... **Platforms**: win **CVEs**: CVE-2013-2347 **Refs**: source, ref1, ref2
HP OpenView Operations OVTrace Buffer Overflow exploit/windows/misc/hp_ovtrace	2007-08-09	average	This module exploits a stack buffer overflo HP OpenView Operations version A.07.50. sending a specially crafted packet, a remot attacker may be able to execute arbitrary c **Platforms**: win **CVEs**: CVE-2007-3872 **Refs**: source
mIRC PRIVMSG Handling Stack Buffer Overflow exploit/windows/misc/mirc_privmsg_server	2008-10-02	normal	This module exploits a buffer overflow in th mIRC IRC Client v6.34 and earlier. By enti mIRC user to connect to this server modul excessively long PRIVMSG command can sent, overwriting ... **Platforms**: win **CVEs**: CVE-2008-4449 **Refs**: source
HTA Web Server exploit/windows/misc/hta_server	2016-10-06	manual	This module hosts an HTML Application (H that when opened will run a payload via Powershell. When a user navigates to the file they will be prompted by IE twice befor payload is executed. **Platforms**: win **Refs**: source, ref1
IBM Cognos tm1admsd.exe Overflow exploit/windows/misc/ibm_cognos_tm1admsd_bof	2012-04-02	normal	This module exploits a stack buffer overflo IBM Cognos Analytic Server Admin service vulnerability exists in the tm1admsd.exe component, due to a dangerous copy of us controlled data to ... **Platforms**: win **CVEs**: CVE-2012-0202 **Refs**: source, ref1
IBM System Director Agent DLL Injection exploit/windows/misc/ibm_director_cim_dllinject	2009-03-10	excellent	This module abuses the "wmicimsv" servic IBM System Director Agent 5.20.3 to accomplish arbitrary DLL injection and exe arbitrary code with SYSTEM privileges. In to accomplish remote ... **Platforms**: win **CVEs**: CVE-2009-0880 **Refs**: source, ref1, ref2
IBM Tivoli Storage Manager Express CAD Service Buffer Overflow exploit/windows/misc/ibm_tsm_cad_ping	2009-11-04	good	This module exploits a stack buffer overflo the IBM Tivoli Storage Manager Express C Service. By sending a "ping" packet contai a long string, an attacker can execute arbit code. NOTE: ... **Platforms**: win **CVEs**: CVE-2009-3853 **Refs**: source
IBM Tivoli Storage Manager Express RCA Service Buffer Overflow exploit/windows/misc/ibm_tsm_rca_dicugetidentify	2009-11-04	great	This module exploits a stack buffer overflo the IBM Tivoli Storage Manager Express Remote Client Agent service. By sending a "dicuGetIdentify" request packet containing long NodeName parameter, ... **Platforms**: win **CVEs**: CVE-2008-4828 **Refs**: source

Metasploit Module	Date	Rank	Details
IBM WebSphere RCE Java Deserialization Vulnerability exploit/windows/misc/ibm_websphere_java_deserialize	2015-11-06	excellent	This module exploits a vulnerability in IBM' WebSphere Application Server. An unsafe deserialization call of unauthenticated Java objects exists to the Apache Commons Collections (ACC) library, ... **Platforms**: win **CVEs**: CVE-2015-7450 **Refs**: source, ref1, ref2, ref3
Borland InterBase isc_attach_database() Buffer Overflow exploit/windows/misc/ib_isc_attach_database	2007-10-03	good	This module exploits a stack buffer overflo Borland InterBase by sending a specially c attach request. **Platforms**: win **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Borland InterBase isc_create_database() Buffer Overflow exploit/windows/misc/ib_isc_create_database	2007-10-03	good	This module exploits a stack buffer overflo Borland InterBase by sending a specially c create request. **Platforms**: win **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Borland InterBase SVC_attach() Buffer Overflow exploit/windows/misc/ib_svc_attach	2007-10-03	good	This module exploits a stack buffer overflo Borland InterBase by sending a specially c service attach request. **Platforms**: win **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Apple iTunes 10 Extended M3U Stack Buffer Overflow exploit/windows/misc/itunes_extm3u_bof	2012-06-21	normal	This module exploits a stack buffer overflo iTunes 10.4.0.80 to 10.6.1.7. When openin extended .m3u file containing an "#EXTINF tag description, iTunes will copy the conter after ... **Platforms**: win **Refs**: source, ref1
LANDesk Management Suite 8.7 Alert Service Buffer Overflow exploit/windows/misc/landesk_aolnsrvr	2007-04-13	average	This module exploits a stack buffer overflo LANDesk Management Suite 8.7. By send an overly long string to the Alert Service, a buffer is overwritten and arbitrary code can executed. **Platforms**: win **CVEs**: CVE-2007-1674 **Refs**: source, ref1
Lianja SQL 1.0.0RC5.1 db_netserver Stack Buffer Overflow exploit/windows/misc/lianja_db_net	2013-05-22	normal	This module exploits a stack buffer overflo the db_netserver process, which is spawne the Lianja SQL server. The issue is fixed in Lianja SQL 1.0.0RC5.2. **Platforms**: win **CVEs**: CVE-2013-3563 **Refs**: source
ManageEngine EventLog Analyzer Remote Code Execution exploit/windows/misc/manageengine_eventlog_analyzer_rce	2015-07-11	manual	This module exploits a SQL query function in ManageEngine EventLog Analyzer v10.6 build 10060 and previous versions. Every authenticated user, including the default "g account can execute ... **Platforms**: win **CVEs**: CVE-2015-7387 **Refs**: source, ref1
Mercury/32 PH Server Module Buffer Overflow exploit/windows/misc/mercury_phonebook	2005-12-19	average	This module exploits a stack-based buffer overflow in Mercury/32 <= v4.01b PH Serv Module. This issue is due to a failure of the application to properly bounds check user-supplied data prior to ... **Platforms**: win **CVEs**: CVE-2005-4411 **Refs**: source
Mini-Stream 3.0.1.1 Buffer Overflow exploit/windows/misc/mini_stream	2009-12-25	normal	This module exploits a stack buffer overflo Mini-Stream 3.0.1.1 By creating a specially crafted pls file, an attacker may be able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2009-5109 **Refs**: source

Metasploit Module	Date	Rank	Details
MS07-064 Microsoft DirectX DirectShow SAMI Buffer Overflow exploit/windows/misc/ms07_064_sami	2007-12-11	normal	This module exploits a stack buffer overflo the DirectShow Synchronized Accessible M Interchanged (SAMI) parser in quartz.dll. T module has only been tested with Windows Media Player ... **Platforms**: win **CVEs**: CVE-2007-3901 **Refs**: source
MS10-104 Microsoft Office SharePoint Server 2007 Remote Code Execution exploit/windows/misc/ms10_104_sharepoint	2010-12-14	excellent	This module exploits a vulnerability found i SharePoint Server 2007 SP2. The software contains a directory traversal, that allows a remote attacker to write arbitrary files to the filesystem, ... **Platforms**: win **CVEs**: CVE-2010-3964 **Refs**: source
Netcat v1.10 NT Stack Buffer Overflow exploit/windows/misc/netcat110_nt	2004-12-27	great	This module exploits a stack buffer overflo Netcat v1.10 NT. By sending an overly long string we are able to overwrite SEH. The vulnerability exists when netcat is used to l (-e) an executable ... **Platforms**: win **CVEs**: CVE-2004-1317 **Refs**: source
NetTransport Download Manager 2.90.510 Buffer Overflow exploit/windows/misc/nettransport	2010-01-02	normal	This exploits a stack buffer overflow in NetTransport Download Manager, part of th NetXfer suite. This module was tested successfully against version 2.90.510. **Platforms**: win **CVEs**: CVE-2017-17968 **Refs**: source
Nvidia Mental Ray Satellite Service Arbitrary DLL Injection exploit/windows/misc/nvidia_mental_ray	2013-12-10	excellent	The Nvidia Mental Ray Satellite Service lis for control commands on port 7414. When receives the command to load a DLL (via a UNC path) it will try to connect back to the on port 7514. ... **Platforms**: win **Refs**: source, ref1
PlugX Controller Stack Buffer Overflow exploit/windows/misc/plugx	2017-07-27	normal	This module exploits a stack buffer overflo the PlugX Controller (C2 server). **Platforms**: win **Refs**: source
Poison Ivy 2.1.x C2 Buffer Overflow exploit/windows/misc/poisonivy_21x_bof	2016-06-03	normal	This module exploits a stack buffer overflo the Poison Ivy 2.1.x C&C server. The explo does not need to know the password chose the bot/server communication. **Platforms**: win **Refs**: source, ref1
Poison Ivy Server Buffer Overflow exploit/windows/misc/poisonivy_bof	2012-06-24	normal	This module exploits a stack buffer overflo the Poison Ivy 2.2.0 to 2.3.2 C&C server. T exploit does not need to know the passwor chosen for the bot/server communication. **Platforms**: win **Refs**: source, ref1, ref2
POP Peeper v3.4 DATE Buffer Overflow exploit/windows/misc/poppeeper_date	2009-02-27	normal	This module exploits a stack buffer overflo POP Peeper v3.4. When a specially crafte DATE string is sent to a client, an attacker be able to execute arbitrary code. This mo is based off ... **Platforms**: win **CVEs**: CVE-2009-1029 **Refs**: source
POP Peeper v3.4 UIDL Buffer Overflow exploit/windows/misc/poppeeper_uidl	2009-02-27	normal	This module exploits a stack buffer overflo POP Peeper v3.4. When a specially crafte UIDL string is sent to a client, an attacker r be able to execute arbitrary code. This mo is based off ... **Platforms**: win **CVEs**: CVE-2009-1029 **Refs**: source

Metasploit Module	Date	Rank	Details
Realtek Media Player Playlist Buffer Overflow exploit/windows/misc/realtek_playlist	2008-12-16	great	This module exploits a stack buffer overflo Realtek Media Player(RtlRack) A4.06. Whe Realtek Media Player client opens a specia crafted playlist, an attacker may be able to execute ... **Platforms**: win **CVEs**: CVE-2008-5664 **Refs**: source
SAP Business One License Manager 2005 Buffer Overflow exploit/windows/misc/sap_2005_license	2009-08-01	great	This module exploits a stack buffer overflo the SAP Business One 2005 License Mana 'NT Naming Service' A and B releases. By sending an excessively long string the stac overwritten enabling ... **Platforms**: win **CVEs**: CVE-2009-4988 **Refs**: source
SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow exploit/windows/misc/sap_netweaver_dispatcher	2012-05-08	normal	This module exploits a stack buffer overflo the SAP NetWeaver Dispatcher service. Th overflow occurs in the DiagTraceR3Info() function and allows a remote attacker to execute arbitrary code by ... **Platforms**: win **CVEs**: CVE-2012-2611 **Refs**: source, ref1, ref2
ShixxNOTE 6.net Font Field Overflow exploit/windows/misc/shixxnote_font	2004-10-04	great	This module exploits a buffer overflow in ShixxNOTE 6.net. The vulnerability is caus due to boundary errors in the handling of fo fields. **Platforms**: win **CVEs**: CVE-2004-1595 **Refs**: source
SolidWorks Workgroup PDM 2014 pdmwService.exe Arbitrary File Write exploit/windows/misc/solidworks_workgroup_pdmwservice_file_write	2014-02-22	good	This module exploits a remote arbitrary file vulnerability in SolidWorks Workgroup PDM 2014 SP2 and prior. For targets running Windows Vista or newer the payload is writ to the startup ... **Platforms**: win **CVEs**: CVE-2014-100015 **Refs**: source
SPlayer 3.7 Content-Type Buffer Overflow exploit/windows/misc/splayer_content_type	2011-05-04	normal	This module exploits a vulnerability in SPla v3.7 or prior. When SPlayer requests the U a media file (video or audio), it is possible t gain arbitrary remote code execution due t buffer ... **Platforms**: win **Refs**: source
CoCSoft StreamDown 6.8.0 Buffer Overflow exploit/windows/misc/stream_down_bof	2011-12-27	good	Stream Down 6.8.0 seh based buffer overf triggered when processing the server resp packet. During the overflow a structured exception handler is overwritten. **Platforms**: win **CVEs**: CVE-2011-5052 **Refs**: source, ref1, ref2
Talkative IRC v0.4.4.16 Response Buffer Overflow exploit/windows/misc/talkative_response	2009-03-17	normal	This module exploits a stack buffer overflo Talkative IRC v0.4.4.16. When a specially crafted response string is sent to a client, a attacker may be able to execute arbitrary c **Platforms**: win **Refs**: source
TinyIdentD 2.2 Stack Buffer Overflow exploit/windows/misc/tiny_identd_overflow	2007-05-14	average	This module exploits a stack based buffer overflow in TinyIdentD version 2.2. If we se long string to the ident service we can over the return address and execute arbitrary co Credit to ... **Platforms**: win **CVEs**: CVE-2007-2711 **Refs**: source

Metasploit Module	Date	Rank	Details
TrendMicro Control Manger CmdProcessor.exe Stack Buffer Overflow exploit/windows/misc/trendmicro_cmdprocessor_addtask	2011-12-07	good	This module exploits a vulnerability in the CmdProcessor.exe component of Trend M Control Manger up to version 5.5. The spe flaw exists within CmdProcessor.exe servic running on TCP port ... **Platforms**: win **CVEs**: CVE-2011-5001 **Refs**: source
UFO: Alien Invasion IRC Client Buffer Overflow exploit/windows/misc/ufo_ai	2009-10-28	average	This module exploits a buffer overflow in th IRC client component of UFO: Alien Invasi 2.2.1. **Platforms**: win **Refs**: source
Veeam ONE Agent .NET Deserialization exploit/windows/misc/veeam_one_agent_deserialization	2020-04-15	normal	This module exploits a .NET deserializatior vulnerability in the Veeam ONE Agent befc the hotfix versions 9.5.5.4587 and 10.0.1.7 the 9 and 10 release lines. Specifically, the module targets ... **Platforms**: win **CVEs**: CVE-2020-10914, CVE-2020-10915 **Refs**: source, ref1
DLL Side Loading Vulnerability in VMware Host Guest Client Redirector exploit/windows/misc/vmhgfs_webdav_dll_sideload	2016-08-05	normal	A DLL side loading vulnerability was found the VMware Host Guest Client Redirector, component of VMware Tools. This issue ca exploited by luring a victim into opening a document from the ... **Platforms**: win **CVEs**: CVE-2016-5330 **Refs**: source, ref1, ref2
Serve DLL via webdav server exploit/windows/misc/webdav_delivery	1999-01-01	manual	This module simplifies the rundll32.exe Application Whitelisting Bypass technique. module creates a webdav server that hosts file. When the user types the provided runc command on a ... **Platforms**: win **Refs**: source
Windows RSH Daemon Buffer Overflow exploit/windows/misc/windows_rsh	2007-07-24	average	This module exploits a vulnerability in Winc RSH daemon 1.8. The vulnerability is due t failure to check for the length of input sent RSH server. A CPORT of 512 -> 1023 mus ... **Platforms**: win **CVEs**: CVE-2007-4006 **Refs**: source
Wireshark console.lua Pre-Loading Script Execution exploit/windows/misc/wireshark_lua	2011-07-18	excellent	This module exploits a vulnerability in Wire 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 parse/execute ... **Platforms**: win **CVEs**: CVE-2011-3360 **Refs**: source, ref1, ref2
Wireshark packet-dect.c Stack Buffer Overflow exploit/windows/misc/wireshark_packet_dect	2011-04-18	good	This module exploits a stack buffer overflo Wireshark <= 1.4.4 by sending a malicious packet. **Platforms**: win **CVEs**: CVE-2011-1591 **Refs**: source, ref1, ref2
Windows Media Services ConnectFunnel Stack Buffer Overflow exploit/windows/mmsp/ms10_025_wmss_connect_funnel	2010-04-13	great	This module exploits a stack buffer overflo the Windows Media Unicast Service versio 4.1.0.3930 (NUMS.exe). By sending a spe crafted FunnelConnect request, an attacke execute ... **Platforms**: win **CVEs**: CVE-2010-0478 **Refs**: source, ref1
Timbuktu Pro Directory Traversal/File Upload exploit/windows/motorola/timbuktu_fileupload	2008-05-10	excellent	This module exploits a directory traversal vulnerability in Motorola's Timbuktu Pro for Windows 8.6.5. **Platforms**: win **CVEs**: CVE-2008-1117 **Refs**: source

Metasploit Module	Date	Rank	Details
Lyris ListManager MSDE Weak sa Password exploit/windows/mssql/lyris_listmanager_weak_pass	2005-12-08	excellent	This module exploits a weak password vulnerability in the Lyris ListManager MSDI install. During installation, the 'sa' account password is set to 'lminstall'. Once the inst completes, it is set ... **Platforms**: win **CVEs**: CVE-2005-4145 **Refs**: source
MS02-039 Microsoft SQL Server Resolution Overflow exploit/windows/mssql/ms02_039_slammer	2002-07-24	good	This is an exploit for the SQL Server 2000 resolution service buffer overflow. This ove is triggered by sending a udp packet to por 1434 which starts with 0x04 and is followe long string ... **Platforms**: win **CVEs**: CVE-2002-0649 **Refs**: source
MS02-056 Microsoft SQL Server Hello Overflow exploit/windows/mssql/ms02_056_hello	2002-08-05	good	By sending malformed data to TCP port 14 an unauthenticated remote attacker could overflow a buffer and possibly execute cod the server with SYSTEM level privileges. T module should work ... **Platforms**: win **CVEs**: CVE-2002-1123 **Refs**: source
MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption exploit/windows/mssql/ms09_004_sp_replwritetovarbin	2008-12-09	good	A heap-based buffer overflow can occur wl calling the undocumented "sp_replwritetov extended stored procedure. This vulnerabi affects all versions of Microsoft SQL Serve 2000 and 2005, ... **Platforms**: win **CVEs**: CVE-2008-5416 **Refs**: source
MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption via SQL Injection exploit/windows/mssql/ms09_004_sp_replwritetovarbin_sqli	2008-12-09	excellent	A heap-based buffer overflow can occur wl calling the undocumented "sp_replwritetov extended stored procedure. This vulnerabi affects all versions of Microsoft SQL Serve 2000 and 2005, ... **Platforms**: win **CVEs**: CVE-2008-5416 **Refs**: source, ref1
Microsoft SQL Server Clr Stored Procedure Payload Execution exploit/windows/mssql/mssql_clr_payload	1999-01-01	excellent	This module executes an arbitrary native payload on a Microsoft SQL server by load custom SQL CLR Assembly into the target installation, and calling it directly with a bas encoded ... **Platforms**: win **Refs**: source, ref1
Microsoft SQL Server Database Link Crawling Command Execution exploit/windows/mssql/mssql_linkcrawler	2000-01-01	great	This module can be used to crawl MS SQL Server database links and deploy Metasplo payloads through links configured with sysadmin privileges using a valid SQL Ser Login. If you are attempting to ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
Microsoft SQL Server Payload Execution exploit/windows/mssql/mssql_payload	2000-05-30	excellent	This module executes an arbitrary payload Microsoft SQL Server by using the "xp_cmdshell" stored procedure. Currently, three delivery methods are supported. Firs original method uses ... **Platforms**: win **CVEs**: CVE-2000-0402, CVE-2000-1209 **Refs**: source
Microsoft SQL Server Payload Execution via SQL Injection exploit/windows/mssql/mssql_payload_sqli	2000-05-30	excellent	This module will execute an arbitrary paylo a Microsoft SQL Server, using a SQL inject vulnerability. Once a vulnerability is identifi this module will use xp_cmdshell to upload execute ... **Platforms**: win **CVEs**: CVE-2000-0402, CVE-2000-1209 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Oracle MySQL for Microsoft Windows MOF Execution exploit/windows/mysql/mysql_mof	2012-12-01	excellent	This module takes advantage of a file privil misconfiguration problem specifically agair Windows MySQL servers (due to the use c .mof file). This may result in arbitrary code execution under ... **Platforms**: win **CVEs**: CVE-2012-5613 **Refs**: source, ref1
Oracle MySQL for Microsoft Windows FILE Privilege Abuse exploit/windows/mysql/mysql_start_up	2012-12-01	excellent	This module takes advantage of a file privil misconfiguration problem specifically agair Windows MySQL servers. This module abu the FILE privilege to write a payload to Microsoft's All Users ... **Platforms**: win **CVEs**: CVE-2012-5613 **Refs**: source, ref1
MySQL yaSSL SSL Hello Message Buffer Overflow exploit/windows/mysql/mysql_yassl_hello	2008-01-04	average	This module exploits a stack buffer overflo the yaSSL (1.7.5 and earlier) implementati bundled with MySQL <= 6.0. By sending a specially crafted Hello packet, an attacker be able to execute ... **Platforms**: win **CVEs**: CVE-2008-0226 **Refs**: source
Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential exploit/windows/mysql/scrutinizer_upload_exec	2012-07-27	excellent	This exploits an insecure config found in Scrutinizer NetFlow sFlow Analyzer. By de the software installs a default password in MySQL, and binds the service to "0.0.0.0". allows any ... **Platforms**: win **CVEs**: CVE-2012-3951 **Refs**: source, ref1, ref2
Omni-NFS Server Buffer Overflow exploit/windows/nfs/xlink_nfsd	2006-11-06	average	This module exploits a stack buffer overflo Xlink Omni-NFS Server 5.2 When sending specially crafted nfs packet, an attacker ma able to execute arbitrary code. **Platforms**: win **CVEs**: CVE-2006-5780 **Refs**: source, ref1
CA Unified Infrastructure Management Nimsoft 7.80 - Remote Buffer Overflow exploit/windows/nimsoft/nimcontroller_bof	2020-02-05	excellent	This module exploits a buffer overflow with CA Unified Infrastructure Management nimcontroller. The vulnerability occurs in th robot (controller) component when sending specially crafted ... **Platforms**: win **CVEs**: CVE-2020-8010, CVE-2020-8012 **Refs**: source, ref1
MS05-030 Microsoft Outlook Express NNTP Response Parsing Buffer Overflow exploit/windows/nntp/ms05_030_nntp	2005-06-14	normal	This module exploits a stack buffer overflo the news reader of Microsoft Outlook Expr **Platforms**: win **CVEs**: CVE-2005-1213 **Refs**: source
NFR Agent FSFUI Record File Upload RCE exploit/windows/novell/file_reporter_fsfui_upload	2012-11-16	great	NFRAgent.exe, a component of Novell File Reporter (NFR), allows remote attackers to upload arbitrary files via a directory travers while handling requests to /FSF/CMD with FSFUI records with UICMD ... **Platforms**: win **CVEs**: CVE-2012-4959 **Refs**: source, ref1
Novell GroupWise Messenger Client Buffer Overflow exploit/windows/novell/groupwisemessenger_client	2008-07-02	normal	This module exploits a stack buffer overflo Novell's GroupWise Messenger Client. By sending a specially crafted HTTP response attacker may be able to execute arbitrary c **Platforms**: win **CVEs**: CVE-2008-2703 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
NetIQ Privileged User Manager 2.3.1 ldapagnt_eval() Remote Perl Code Execution exploit/windows/novell/netiq_pum_eval	2012-11-15	excellent	This module abuses a lack of authorization the NetIQ Privileged User Manager service (unifid.exe) to execute arbitrary perl code. problem exists in the ldapagnt module. The module has been ... **Platforms**: win **CVEs**: CVE-2012-5932 **Refs**: source
Novell NetMail NMAP STOR Buffer Overflow exploit/windows/novell/nmap_stor	2006-12-23	average	This module exploits a stack buffer overflo Novell's Netmail 3.52 NMAP STOR verb. B sending an overly long string, an attacker c overwrite the buffer and control program execution. **Platforms**: win **CVEs**: CVE-2006-6424 **Refs**: source
Novell ZENworks 6.5 Desktop/Server Management Overflow exploit/windows/novell/zenworks_desktop_agent	2005-05-19	good	This module exploits a heap overflow in the Novell ZENworks Desktop Management ag This vulnerability was discovered by Alex Wheeler. **Platforms**: win **CVEs**: CVE-2005-1543 **Refs**: source
Novell ZENworks Configuration Management Preboot Service 0x21 Buffer Overflow exploit/windows/novell/zenworks_preboot_op21_bof	2010-03-30	normal	This module exploits a remote buffer overfl the ZENworks Configuration Management SP2. The vulnerability exists in the Preboo service and can be triggered by sending a specially crafted ... **Platforms**: win **CVEs**: CVE-2012-2215 **Refs**: source, ref1
Novell ZENworks Configuration Management Preboot Service 0x4c Buffer Overflow exploit/windows/novell/zenworks_preboot_op4c_bof	2012-02-22	normal	This module exploits a remote buffer overfl the ZENworks Configuration Management. vulnerability exists in the Preboot service a can be triggered by sending a specially cra packet with ... **Platforms**: win **CVEs**: CVE-2011-3176 **Refs**: source, ref1
Novell ZENworks Configuration Management Preboot Service 0x6c Buffer Overflow exploit/windows/novell/zenworks_preboot_op6c_bof	2012-02-22	normal	This module exploits a remote buffer overfl the ZENworks Configuration Management. vulnerability exists in the Preboot service a can be triggered by sending a specially cra packet with ... **Platforms**: win **CVEs**: CVE-2011-3175 **Refs**: source, ref1
Novell ZENworks Configuration Management Preboot Service 0x06 Buffer Overflow exploit/windows/novell/zenworks_preboot_op6_bof	2010-03-30	normal	This module exploits a remote buffer overfl the ZENworks Configuration Management SP2. The vulnerability exists in the Preboo service and can be triggered by sending a specially crafted ... **Platforms**: win **Refs**: source, ref1
Nuuo Central Management Server Authenticated Arbitrary File Upload exploit/windows/nuuo/nuuo_cms_fu	2018-10-11	manual	The COMMITCONFIG verb is used by a C client to upload and modify the configuratic the CMS Server. The vulnerability is in the "FileName" parameter, which accepts direc traversal (.\.\) ... **Platforms**: win **CVEs**: CVE-2018-17936 **Refs**: source, ref1, ref2, ref3
Nuuo Central Management Authenticated SQL Server SQLi exploit/windows/nuuo/nuuo_cms_sqli	2018-10-11	normal	The Nuuo Central Management Server allc an authenticated user to query the state of alarms. This functionality can be abused to inject SQL into the query. As SQL Server 2 Express is ... **Platforms**: win **CVEs**: CVE-2018-18982 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Oracle Database Client System Analyzer Arbitrary File Upload exploit/windows/oracle/client_system_analyzer_upload	2011-01-18	excellent	This module exploits an arbitrary file uploa vulnerability on the Client Analyzer compor as included in Oracle Database 11g, which allows remote attackers to upload and exe arbitrary code. ... **Platforms**: win **CVEs**: CVE-2010-3600 **Refs**: source, ref1
Oracle Job Scheduler Named Pipe Command Execution exploit/windows/oracle/extjob	2007-01-01	excellent	This module exploits the Oracle Job Schec to execute arbitrary commands. The Job Scheduler is implemented via the compone extjob.exe which listens on a named pipe c "orcljsex" and ... **Platforms**: win **Refs**: source, ref1
Oracle Secure Backup NDMP_CONNECT_CLIENT_AUTH Buffer Overflow exploit/windows/oracle/osb_ndmp_auth	2009-01-14	good	The module exploits a stack buffer overflov Oracle Secure Backup. When sending a specially crafted NDMP_CONNECT_CLIENT_AUTH packe attacker may be able to execute arbitrary c **Platforms**: win **CVEs**: CVE-2008-5444 **Refs**: source, ref1
Oracle 8i TNS Listener (ARGUMENTS) Buffer Overflow exploit/windows/oracle/tns_arguments	2001-06-28	good	This module exploits a stack buffer overflov Oracle 8i. When sending a specially crafte packet containing an overly long ARGUME string to the TNS service, an attacker may able to execute ... **Platforms**: win **CVEs**: CVE-2001-0499 **Refs**: source
Oracle 10gR2 TNS Listener AUTH_SESSKEY Buffer Overflow exploit/windows/oracle/tns_auth_sesskey	2009-10-20	great	This module exploits a stack buffer overflov Oracle. When sending a specially crafted p containing a long AUTH_SESSKEY value TNS service, an attacker may be able to execute arbitrary ... **Platforms**: win **CVEs**: CVE-2009-1979 **Refs**: source, ref1, ref2, ref3
Oracle 8i TNS Listener SERVICE_NAME Buffer Overflow exploit/windows/oracle/tns_service_name	2002-05-27	good	This module exploits a stack buffer overflov Oracle. When sending a specially crafted p containing a long SERVICE_NAME to the service, an attacker may be able to execut arbitrary code. **Platforms**: win **CVEs**: CVE-2002-0965 **Refs**: source, ref1
Seattle Lab Mail 5.5 POP3 Buffer Overflow exploit/windows/pop3/seattlelab_pass	2003-05-07	great	There exists an unauthenticated buffer ove vulnerability in the POP3 server of Seattle Mail 5.5 when sending a password with excessive length. Successful exploitation s not crash either ... **Platforms**: win **CVEs**: CVE-2003-0264 **Refs**: source
PostgreSQL for Microsoft Windows Payload Execution exploit/windows/postgres/postgres_payload	2009-04-10	excellent	On default Microsoft Windows installations PostgreSQL the postgres service account write to the current directory (which is usua "C:Program FilesPostgreSQLdata" where i **Platforms**: win **Refs**: source, ref1
Blue Coat WinProxy Host Header Overflow exploit/windows/proxy/bluecoat_winproxy_host	2005-01-05	great	This module exploits a buffer overflow in th Blue Coat Systems WinProxy service by sending a long port value for the Host heac a HTTP request. **Platforms**: win **CVEs**: CVE-2005-4085 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
CCProxy Telnet Proxy Ping Overflow exploit/windows/proxy/ccproxy_telnet_ping	2004-11-11	average	This module exploits the YoungZSoft CCPr <= v6.2 suite Telnet service. The stack is overwritten when sending an overly long address to the 'ping' command. **Platforms**: win **CVEs**: CVE-2004-2416 **Refs**: source
Proxy-Pro Professional GateKeeper 4.7 GET Request Overflow exploit/windows/proxy/proxypro_http_get	2004-02-23	great	This module exploits a stack buffer overflo Proxy-Pro Professional GateKeeper 4.7. B sending a long HTTP GET to the default pc 3128, a remote attacker could overflow a b and execute ... **Platforms**: win **CVEs**: CVE-2004-0326 **Refs**: source
Qbik WinGate WWW Proxy Server URL Processing Overflow exploit/windows/proxy/qbik_wingate_wwwproxy	2006-06-07	good	This module exploits a stack buffer overflo Qbik WinGate version 6.1.1.1077 and earli sending malformed HTTP POST URL to th HTTP proxy service on port 80, a remote attacker could overflow ... **Platforms**: win **CVEs**: CVE-2006-2926 **Refs**: source
CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free exploit/windows/rdp/cve_2019_0708_bluekeep_rce	2019-05-14	manual	The RDP termdd.sys driver improperly han binds to internal-only channel MS_T120, allowing a malformed Disconnect Provider Indication message to cause use-after-free With a controllable data/size ... **Platforms**: win **CVEs**: CVE-2019-0708 **Refs**: source, ref1, ref2
RDP DOUBLEPULSAR Remote Code Execution exploit/windows/rdp/rdp_doublepulsar_rce	2017-04-14	great	This module executes a Metasploit payloa against the Equation Group's DOUBLEPUI implant for RDP. While this module primari performs code execution against the impla the "Neutralize implant" ... **Platforms**: win **Refs**: source, ref1
7-Technologies IGSS 9 Data Server/Collector Packet Handling Vulnerabilities exploit/windows/scada/igss9_misc	2011-03-24	excellent	This module exploits multiple vulnerabilitie found on IGSS 9's Data Server and Data Collector services. The initial approach is f transferring our binary with Write packets (opcode 0x0D) via ... **Platforms**: win **CVEs**: CVE-2011-1565, CVE-2011-1566 **Refs**: source, ref1, ref2, ref3
ABB MicroSCADA wserver.exe Remote Code Execution exploit/windows/scada/abb_wserver_exec	2013-04-05	excellent	This module exploits a remote stack buffer overflow vulnerability in ABB MicroSCADA issue is due to the handling of unauthentica EXECUTE operations on the wserver.exe component, which allows ... **Platforms**: win **CVEs**: CVE-2019-5620 **Refs**: source, ref1
Advantech WebAccess Dashboard Viewer uploadImageCommon Arbitrary File Upload exploit/windows/scada/advantech_webaccess_dashboard_file_upload	2016-02-05	excellent	This module exploits an arbitrary file uploa vulnerability found in Advantech WebAcces 8.0. This vulnerability allows remote attack execute arbitrary code on vulnerable installations of ... **Platforms**: win **CVEs**: CVE-2016-0854 **Refs**: source, ref1
Advantech WebAccess Webvrpcs Service Opcode 80061 Stack Buffer Overflow exploit/windows/scada/advantech_webaccess_webvrpcs_bof	2017-11-02	good	This module exploits a stack buffer overflo Advantech WebAccess 8.2. By sending a specially crafted DCERPC request, an atta could overflow the buffer and execute arbit code. **Platforms**: win **CVEs**: CVE-2017-14016 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
CitectSCADA/CitectFacilities ODBC Buffer Overflow exploit/windows/scada/citect_scada_odbc	2008-06-11	normal	This module exploits a stack buffer overflo CitectSCADA's ODBC daemon. This has o been tested against Citect v5, v6 and v7. **Platforms**: win **CVEs**: CVE-2008-2639 **Refs**: source, ref1, ref2, ref3
SCADA 3S CoDeSys Gateway Server Directory Traversal exploit/windows/scada/codesys_gateway_server_traversal	2013-02-02	excellent	This module exploits a directory traversal vulnerability that allows arbitrary file creatic which can be used to execute a mof file in to gain remote execution within the SCADA system. **Platforms**: win **CVEs**: CVE-2012-4705 **Refs**: source, ref1
SCADA 3S CoDeSys CmpWebServer Stack Buffer Overflow exploit/windows/scada/codesys_web_server	2011-12-02	normal	This module exploits a remote stack buffer overflow vulnerability in 3S-Smart Software Solutions product CoDeSys Scada Web Se Version 1.1.9.9. This vulnerability affects versions 3.4 SP4 Patch 2 ... **Platforms**: win **CVEs**: CVE-2011-5007 **Refs**: source, ref1, ref2, ref3
DaqFactory HMI NETB Request Overflow exploit/windows/scada/daq_factory_bof	2011-09-13	good	This module exploits a stack buffer overflo Azeotech's DaqFactory product. The speci vulnerability is triggered when sending a specially crafted 'NETB' request to port 20(Exploitation of ... **Platforms**: win **CVEs**: CVE-2011-3492 **Refs**: source, ref1, ref2
Delta Electronics Delta Industrial Automation COMMGR 1.08 Stack Buffer Overflow exploit/windows/scada/delta_ia_commgr_bof	2018-07-02	normal	This module exploits a stack based buffer overflow in Delta Electronics Delta Industri Automation COMMGR 1.08. The vulnerabi exists in COMMGR.exe when handling spe crafted packets. This ... **Platforms**: win **CVEs**: CVE-2018-10594 **Refs**: source, ref1
Siemens FactoryLink 8 CSService Logging Path Param Buffer Overflow exploit/windows/scada/factorylink_csservice	2011-03-25	normal	This module exploits a vulnerability found c Siemens FactoryLink 8. The vulnerability o when CSService.exe processes a CSMSG_ListFiles_REQ message, the use supplied path first gets converted ... **Platforms**: win **Refs**: source, ref1, ref2
Siemens FactoryLink vrn.exe Opcode 9 Buffer Overflow exploit/windows/scada/factorylink_vrn_09	2011-03-21	average	This module exploits a stack buffer overflo FactoryLink 7.5, 7.5 SP2, and 8.0.1.703. B sending a specially crafted packet, an attac may be able to execute arbitrary code due the improper ... **Platforms**: win **Refs**: source, ref1, ref2
GE Proficy CIMPLICITY gefebt.exe Remote Code Execution exploit/windows/scada/ge_proficy_cimplicity_gefebt	2014-01-23	excellent	This module abuses the gefebt.exe compo in GE Proficy CIMPLICITY, reachable throu the CIMPLICIY CimWebServer. The vulner component allows to execute remote BCL in shared resources. An ... **Platforms**: win **CVEs**: CVE-2014-0750 **Refs**: source, ref1
Iconics GENESIS32 Integer Overflow Version 9.21.201.01 exploit/windows/scada/iconics_genbroker	2011-03-21	good	The GenBroker service on port 38080 is affected by three integer overflow vulnerab while handling opcode 0x4b0, which is cau by abusing the the memory allocations nee for the number of ... **Platforms**: win **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
ICONICS WebHMI ActiveX Buffer Overflow exploit/windows/scada/iconics_webhmi_setactivexguid	2011-05-05	good	This module exploits a vulnerability found i ICONICS WebHMI's ActiveX control. By supplying a long string of data to the 'SetActiveXGUID' parameter, GenVersion.d fails to do any proper bounds ... **Platforms**: win **CVEs**: CVE-2011-2089 **Refs**: source, ref1, ref2
7-Technologies IGSS IGSSdataServer.exe Stack Buffer Overflow exploit/windows/scada/igss9_igssdataserver_listall	2011-03-24	good	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 comma the application fails to do proper ... **Platforms**: win **CVEs**: CVE-2011-1567 **Refs**: source, ref1, ref2
7-Technologies IGSS 9 IGSSdataServer .RMS Rename Buffer Overflow exploit/windows/scada/igss9_igssdataserver_rename	2011-03-24	normal	This module exploits a vulnerability found c Technologies IGSS 9. By supplying a long of data to the 'Rename' (0x02), 'Delete' (0x or 'Add' (0x04) command, a buffer overflow condition ... **Platforms**: win **CVEs**: CVE-2011-1567 **Refs**: source, ref1, ref2
Interactive Graphical SCADA System Remote Command Injection exploit/windows/scada/igss_exec_17	2011-03-21	excellent	This module abuses a directory traversal fl Interactive Graphical SCADA System v9.0(conjunction with the traversal flaw, if opcod 0x17 is sent to the dc.exe process, an atta may be ... **Platforms**: win **CVEs**: CVE-2011-1566 **Refs**: source, ref1
InduSoft Web Studio Arbitrary Upload Remote Code Execution exploit/windows/scada/indusoft_webstudio_exec	2011-11-04	excellent	This module exploits a lack of authenticatic and authorization on the InduSoft Web Stu Remote Agent, that allows a remote attack write arbitrary files to the filesystem, by abu the ... **Platforms**: win **CVEs**: CVE-2011-4051 **Refs**: source
MOXA Device Manager Tool 2.1 Buffer Overflow exploit/windows/scada/moxa_mdmtool	2010-10-20	great	This module exploits a stack buffer overflo MOXA MDM Tool 2.1. When sending a spe crafted MDMGw (MDM2_Gateway) respon an attacker may be able to execute arbitrai code. **Platforms**: win **CVEs**: CVE-2010-4741 **Refs**: source, ref1, ref2
Procyon Core Server HMI Coreservice.exe Stack Buffer Overflow exploit/windows/scada/procyon_core_server	2011-09-08	normal	This module exploits a vulnerability in the coreservice.exe component of Proycon Co Server <= v1.13. While processing a passv the application fails to do proper bounds checking before copying ... **Platforms**: win **CVEs**: CVE-2011-3322 **Refs**: source, ref1
DATAC RealWin SCADA Server Buffer Overflow exploit/windows/scada/realwin	2008-09-26	great	This module exploits a stack buffer overflo DATAC Control International RealWin SCA Server 2.0 (Build 6.0.10.37). By sending a specially crafted FC_INFOTAG/SET_CON packet, an attacker may ... **Platforms**: win **CVEs**: CVE-2008-4322 **Refs**: source
RealWin SCADA Server DATAC Login Buffer Overflow exploit/windows/scada/realwin_on_fcs_login	2011-03-21	great	This module exploits a stack buffer overflo DATAC Control International RealWin SCA Server 2.1 (Build 6.0.10.10) or earlier. By sending a specially crafted On_FC_CONNECT_FCS_LOGIN packet . **Platforms**: win **CVEs**: CVE-2011-1563 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
DATAC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow exploit/windows/scada/realwin_on_fc_binfile_a	2011-03-21	great	This module exploits a vulnerability found i DATAC Control International RealWin SCA Server 2.1 and below. By supplying a spec crafted On_FC_BINFILE_FCS_*FILE pack port 910, RealWin ... **Platforms**: win **CVEs**: CVE-2011-1563 **Refs**: source, ref1, ref2
DATAC RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow exploit/windows/scada/realwin_scpc_initialize	2010-10-15	great	This module exploits a stack buffer overflo DATAC Control International RealWin SCA Server 2.0 (Build 6.1.8.10). By sending a specially crafted packet, an attacker may b able to execute ... **Platforms**: win **CVEs**: CVE-2010-4142 **Refs**: source, ref1, ref2
DATAC RealWin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow exploit/windows/scada/realwin_scpc_initialize_rf	2010-10-15	great	This module exploits a stack buffer overflo DATAC Control International RealWin SCA Server 2.0 (Build 6.1.8.10). By sending a specially crafted packet, an attacker may b able to execute ... **Platforms**: win **CVEs**: CVE-2010-4142 **Refs**: source, ref1, ref2
DATAC RealWin SCADA Server SCPC_TXTEVENT Buffer Overflow exploit/windows/scada/realwin_scpc_txtevent	2010-11-18	great	This module exploits a stack buffer overflo DATAC Control International RealWin SCA Server 2.0 (Build 6.1.8.10). By sending a specially crafted packet, an attacker may b able to execute ... **Platforms**: win **CVEs**: CVE-2010-4142 **Refs**: source
Rockwell FactoryTalk View SE SCADA Unauthenticated Remote Code Execution exploit/windows/scada/rockwell_factorytalk_rce	2020-06-22	excellent	This module exploits a series of vulnerabili to achieve unauthenticated remote code execution on the Rockwell FactoryTalk Vie SCADA product as the IIS user. The attack relies on the chaining ... **Platforms**: win **CVEs**: CVE-2020-12027, CVE-2020-1202 CVE-2020-12029 **Refs**: source, ref1, ref2, ref3
Measuresoft ScadaPro Remote Command Execution exploit/windows/scada/scadapro_cmdexe	2011-09-16	excellent	This module allows remote attackers to ex arbitrary commands on the affected systen abusing via Directory Traversal attack whe using the 'xf' command (execute function). attacker can ... **Platforms**: win **CVEs**: CVE-2011-3497 **Refs**: source, ref1, ref2, ref3
Sunway Forcecontrol SNMP NetDBServer.exe Opcode 0x57 exploit/windows/scada/sunway_force_control_netdbsrv	2011-09-22	great	This module exploits a stack based buffer overflow found in the SNMP NetDBServer service of Sunway Forcecontrol <= 6.1 sp3 overflow is triggered when sending an ove long string to the ... **Platforms**: win **Refs**: source, ref1
Sielco Sistemi Winlog Buffer Overflow exploit/windows/scada/winlog_runtime	2011-01-13	great	This module exploits a buffer overflow in S Sistem Winlog <= 2.07.00. When sending a specially formatted packet to the Runtime.e service, an attacker may be able to execut arbitrary code. **Platforms**: win **CVEs**: CVE-2011-0517 **Refs**: source, ref1, ref2
Sielco Sistemi Winlog Buffer Overflow 2.07.14 - 2.07.16 exploit/windows/scada/winlog_runtime_2	2012-06-04	normal	This module exploits a buffer overflow in S Sistem Winlog <= 2.07.16. When sending a specially formatted packet to the Runtime.e service on port 46824, an attacker may be to execute ... **Platforms**: win **CVEs**: CVE-2012-3815 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Yokogawa CENTUM CS 3000 BKBCopyD.exe Buffer Overflow exploit/windows/scada/yokogawa_bkbcopyd_bof	2014-03-10	normal	This module exploits a stack based buffer overflow in Yokogawa CENTUM CS 3000. vulnerability exists in the service BKBCopyD.exe when handling specially cr packets. This module has been ... **Platforms**: win **CVEs**: CVE-2014-0784 **Refs**: source, ref1, ref2
Yokogawa CS3000 BKESimmgr.exe Buffer Overflow exploit/windows/scada/yokogawa_bkesimmgr_bof	2014-03-10	normal	This module exploits an stack based buffer overflow on Yokogawa CS3000. The vulnerability exists in the BKESimmgr.exe service when handling specially crafted pa due to an insecure usage of ... **Platforms**: win **CVEs**: CVE-2014-0782 **Refs**: source, ref1, ref2
Yokogawa CS3000 BKFSim_vhfd.exe Buffer Overflow exploit/windows/scada/yokogawa_bkfsim_vhfd	2014-05-23	normal	This module exploits a stack based buffer overflow on Yokogawa CS3000. The vulnerability exists in the service BKFSim_vhfd.exe when using malicious us controlled data to create logs using functio **Platforms**: win **CVEs**: CVE-2014-3888 **Refs**: source, ref1, ref2, ref3
Yokogawa CENTUM CS 3000 BKHOdeq.exe Buffer Overflow exploit/windows/scada/yokogawa_bkhodeq_bof	2014-03-10	average	This module exploits a stack based buffer overflow in Yokogawa CENTUM CS 3000. vulnerability exists in the service BKHOdeq when handling specially crafted packets. T module has been tested ... **Platforms**: win **CVEs**: CVE-2014-0783 **Refs**: source, ref1, ref2
AIM Triton 1.0.4 CSeq Buffer Overflow exploit/windows/sip/aim_triton_cseq	2006-07-10	great	This module exploits a buffer overflow in A AIM Triton 1.0.4. By sending an overly long CSeq value, a remote attacker could overfl buffer and execute arbitrary code on the sy with the ... **Platforms**: win **CVEs**: CVE-2006-3524 **Refs**: source
SIPfoundry sipXezPhone 0.35a CSeq Field Overflow exploit/windows/sip/sipxezphone_cseq	2006-07-10	great	This module exploits a buffer overflow in SIPfoundry's sipXezPhone version 0.35a. I sending an long CSeq header, a remote attacker could overflow a buffer and execu arbitrary code on the system ... **Platforms**: win **CVEs**: CVE-2006-3524 **Refs**: source
SIPfoundry sipXphone 2.6.0.27 CSeq Buffer Overflow exploit/windows/sip/sipxphone_cseq	2006-07-10	great	This module exploits a buffer overflow in SIPfoundry's sipXphone 2.6.0.27. By sendi overly long CSeq value, a remote attacker overflow a buffer and execute arbitrary cod the system ... **Platforms**: win **CVEs**: CVE-2006-3524 **Refs**: source
Generic DLL Injection From Shared Resource exploit/windows/smb/generic_smb_dll_injection	2015-03-04	manual	This is a general-purpose module for explo conditions where a DLL can be loaded fron specified SMB share. This module serves payloads as DLLs over an SMB service. **Platforms**: win **Refs**: source
Group Policy Script Execution From Shared Resource exploit/windows/smb/group_policy_startup	2015-01-26	manual	This is a general-purpose module for explo systems with Windows Group Policy config to load VBS startup/logon scripts from rem locations. This module runs a SMB shared resource that will ... **Platforms**: win **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
IPass Control Pipe Remote Command Execution exploit/windows/smb/ipass_pipe_exec	2015-01-21	excellent	This module exploits a vulnerability in the I Client service. This service provides a nam pipe which can be accessed by the user gr BUILTINUsers. This pipe can be abused to the service ... **Platforms**: win **CVEs**: CVE-2015-0925 **Refs**: source, ref1
MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow exploit/windows/smb/ms03_049_netapi	2003-11-11	good	This module exploits a stack buffer overflo the NetApi32 NetAddAlternateComputerNa function using the Workstation service in Windows XP. **Platforms**: win **CVEs**: CVE-2003-0812 **Refs**: source
MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow exploit/windows/smb/ms04_007_killbill	2004-02-10	low	This is an exploit for a previously undisclos vulnerability in the bit string decoding code the Microsoft ASN.1 library. This vulnerabil not related to the bit string vulnerability ... **Platforms**: win **CVEs**: CVE-2003-0818 **Refs**: source
MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow exploit/windows/smb/ms04_011_lsass	2004-04-13	good	This module exploits a stack buffer overflo the LSASS service, this vulnerability was originally found by eEye. When re-exploitin Windows XP system, you will need need to this module ... **Platforms**: win **CVEs**: CVE-2003-0533 **Refs**: source
MS04-031 Microsoft NetDDE Service Overflow exploit/windows/smb/ms04_031_netdde	2004-10-12	good	This module exploits a stack buffer overflo the NetDDE service, which is the precurso the DCOM interface. This exploit effects or operating systems released prior to Windo XP SP1 (2000 ... **Platforms**: win **CVEs**: CVE-2004-0206 **Refs**: source
MS05-039 Microsoft Plug and Play Service Overflow exploit/windows/smb/ms05_039_pnp	2005-08-09	good	This module exploits a stack buffer overflo the Windows Plug and Play service. This vulnerability can be exploited on Windows without a valid user account. NOTE: Since PnP service runs ... **Platforms**: win **CVEs**: CVE-2005-1983 **Refs**: source
MS06-025 Microsoft RRAS Service RASMAN Registry Overflow exploit/windows/smb/ms06_025_rasmans_reg	2006-06-13	good	This module exploits a registry-based stacl buffer overflow in the Windows Routing an Remote Access Service. Since the service hosted inside svchost.exe, a failed exploit attempt can cause other ... **Platforms**: win **CVEs**: CVE-2006-2370 **Refs**: source
MS06-025 Microsoft RRAS Service Overflow exploit/windows/smb/ms06_025_rras	2006-06-13	average	This module exploits a stack buffer overflo the Windows Routing and Remote Access Service. Since the service is hosted inside svchost.exe, a failed exploit attempt can ca other system services ... **Platforms**: win **CVEs**: CVE-2006-2370 **Refs**: source
MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow exploit/windows/smb/ms06_040_netapi	2006-08-08	good	This module exploits a stack buffer overflo the NetApi32 CanonicalizePathName() fun using the NetpwPathCanonicalize RPC cal the Server Service. It is likely that other RF calls could be ... **Platforms**: win **CVEs**: CVE-2006-3439 **Refs**: source

Metasploit Module	Date	Rank	Details
MS06-066 Microsoft Services nwapi32.dll Module Exploit exploit/windows/smb/ms06_066_nwapi	2006-11-14	good	This module exploits a stack buffer overflo the svchost service when the netware clier service is running. This specific vulnerabilit in the nwapi32.dll module. **Platforms**: win **CVEs**: CVE-2006-4688 **Refs**: source
MS06-066 Microsoft Services nwwks.dll Module Exploit exploit/windows/smb/ms06_066_nwwks	2006-11-14	good	This module exploits a stack buffer overflo the svchost service, when the netware clie service is running. This specific vulnerabilit in the nwapi32.dll module. **Platforms**: win **CVEs**: CVE-2006-4688 **Refs**: source
MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow exploit/windows/smb/ms06_070_wkssvc	2006-11-14	manual	This module exploits a stack buffer overflo the NetApi32 NetpManageIPCConnect fun using the Workstation service in Windows SP4 and Windows XP SP2. In order to exp this ... **Platforms**: win **CVEs**: CVE-2006-4691 **Refs**: source
MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB) exploit/windows/smb/ms07_029_msdns_zonename	2007-04-12	manual	This module exploits a stack buffer overflo the RPC interface of the Microsoft DNS se The vulnerability is triggered when a long z name parameter is supplied that contains escaped octal ... **Platforms**: win **CVEs**: CVE-2007-1748 **Refs**: source
MS08-067 Microsoft Server Service Relative Path Stack Corruption exploit/windows/smb/ms08_067_netapi	2008-10-28	great	This module exploits a parsing flaw in the p canonicalization code of NetAPI32.dll throu the Server Service. This module is capable bypassing NX on some operating systems service packs. ... **Platforms**: win **Refs**: source, ref1
MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference exploit/windows/smb/ms09_050_smb2_negotiate_func_index	2009-09-07	good	This module exploits an out of bounds func table dereference in the SMB request valid code of the SRV2.SYS driver included with Windows Vista, Windows 7 release candid (not RTM), and ... **Platforms**: win **CVEs**: CVE-2009-3103 **Refs**: source, ref1
Microsoft Windows Shell LNK Code Execution exploit/windows/smb/ms10_046_shortcut_icon_dllloader	2010-07-16	excellent	This module exploits a vulnerability in the handling of Windows Shortcut files (.LNK) contain an icon resource pointing to a mali DLL. This creates an SMB resource to pro the payload ... **Platforms**: win **CVEs**: CVE-2010-2568 **Refs**: source, ref1
MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability exploit/windows/smb/ms10_061_spoolss	2010-09-14	excellent	This module exploits the RPC service impersonation vulnerability detailed in Micr Bulletin MS10-061. By making a specific D RPC request to the StartDocPrinter proced an attacker can ... **Platforms**: win **CVEs**: CVE-2010-2729 **Refs**: source
Microsoft Windows Shell LNK Code Execution exploit/windows/smb/ms15_020_shortcut_icon_dllloader	2015-03-10	excellent	This module exploits a vulnerability in the MS10-046 patch to abuse (again) the hanc of Windows Shortcut files (.LNK) that conta icon resource pointing to a malicious DLL. creates an ... **Platforms**: win **CVEs**: CVE-2015-0096 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	This module is a port of the Equation Grou ETERNALBLUE exploit, part of the FuzzBu toolkit released by Shadow Brokers. There buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size ... **Platforms**: win **CVEs**: CVE-2017-0143, CVE-2017-0144, 2017-0145, CVE-2017-0146, CVE-2017-0 CVE-2017-0148 **Refs**: source, ref1
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	This module will exploit SMB with vulnerab in MS17-010 to achieve a write-what-wher primitive. This will then be used to overwrit connection session information with as an Administrator ... **Platforms**: win **CVEs**: CVE-2017-0143, CVE-2017-0146, 2017-0147 **Refs**: source, ref1, ref2, ref3
Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow exploit/windows/smb/netidentity_xtierrpcpipe	2009-04-06	great	This module exploits a stack buffer overflo Novell's NetIdentity Agent. When sending a specially crafted string to the 'XTIERRPCP named pipe, an attacker may be able to ex arbitrary ... **Platforms**: win **CVEs**: CVE-2009-1350 **Refs**: source, ref1
Microsoft Windows Authenticated User Code Execution exploit/windows/smb/psexec	1999-01-01	manual	This module uses a valid administrator username and password (or password has execute an arbitrary payload. This module similar to the "psexec" utility provided by SysInternals. This module ... **Platforms**: win **CVEs**: CVE-1999-0504 **Refs**: source, ref1, ref2, ref3
SMB Delivery exploit/windows/smb/smb_delivery	2016-07-26	excellent	This module serves payloads via an SMB s and provides commands to retrieve and ex the generated payloads. Currently supports DLLs and Powershell. **Platforms**: win **Refs**: source, ref1
SMB DOUBLEPULSAR Remote Code Execution exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	This module executes a Metasploit payload against the Equation Group's DOUBLEPUL implant for SMB as popularly deployed by ETERNALBLUE. While this module primar performs code execution against ... **Platforms**: win **CVEs**: CVE-2017-0143, CVE-2017-0144, 2017-0145, CVE-2017-0146, CVE-2017-0 CVE-2017-0148 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref
MS08-068 Microsoft Windows SMB Relay Code Execution exploit/windows/smb/smb_relay	2001-03-31	excellent	This module will relay SMB authentication requests to another host, gaining access to authenticated SMB session if successful. If connecting user is an administrator and ne logins are ... **Platforms**: win **CVEs**: CVE-2008-4037 **Refs**: source, ref1, ref2, ref3
Microsoft Windows RRAS Service MIBEntryGet Overflow exploit/windows/smb/smb_rras_erraticgopher	2017-06-13	average	This module exploits an overflow in the Windows Routing and Remote Access Ser (RRAS) to execute code as SYSTEM. The RRAS DCERPC endpoint is accessible to unauthenticated users via SMBv1 browser **Platforms**: win **CVEs**: CVE-2017-8461 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref ref7, ref8, ref9, ref10

Metasploit Module	Date	Rank	Details
Timbuktu PlughNTCommand Named Pipe Buffer Overflow exploit/windows/smb/timbuktu_plughntcommand_bof	2009-06-25	great	This module exploits a stack based buffer overflow in Timbuktu Pro version <= 8.6.6 i pretty novel way. This exploit requires two connections. The first connection is used t stack data using ... **Platforms**: win **CVEs**: CVE-2009-1394 **Refs**: source, ref1
WebExec Authenticated User Code Execution exploit/windows/smb/webexec	2018-10-24	manual	This module uses a valid username and password of any level (or password hash) t execute an arbitrary payload. This module similar to the "psexec" module, except allo any non-guest account by ... **Platforms**: win **CVEs**: CVE-2018-15442 **Refs**: source, ref1
TABS MailCarrier v2.51 SMTP EHLO Overflow exploit/windows/smtp/mailcarrier_smtp_ehlo	2004-10-26	good	This module exploits the MailCarrier v2.51 SMTP service. The stack is overwritten wh sending an overly long EHLO command. **Platforms**: win **CVEs**: CVE-2004-1638 **Refs**: source
Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow exploit/windows/smtp/mercury_cram_md5	2007-08-18	great	This module exploits a stack buffer overflo Mercury Mail Transport System 4.51. By sending a specially crafted argument to the AUTH CRAM-MD5 command, an attacker be able to execute arbitrary ... **Platforms**: win **CVEs**: CVE-2007-4440 **Refs**: source
MS03-046 Exchange 2000 XEXCH50 Heap Overflow exploit/windows/smtp/ms03_046_exchange2000_xexch50	2003-10-15	good	This is an exploit for the Exchange 2000 he overflow. Due to the nature of the vulnerab this exploit is not very reliable. This module been tested against Exchange 2000 SP0 a SP3 ... **Platforms**: win **CVEs**: CVE-2003-0714 **Refs**: source
NJStar Communicator 3.00 MiniSMTP Buffer Overflow exploit/windows/smtp/njstar_smtp_bof	2011-10-31	normal	This module exploits a stack buffer overflo vulnerability in NJStar Communicator Vers 3.00 MiniSMTP server. The MiniSMTP application can be seen in multiple NJStar products, and will continue to ... **Platforms**: win **CVEs**: CVE-2011-4040 **Refs**: source, ref1
SysGauge SMTP Validation Buffer Overflow exploit/windows/smtp/sysgauge_client_bof	2017-02-28	normal	This module will setup an SMTP server expecting a connection from SysGauge 1.5 via its SMTP server validation. The module sends a malicious response along in the 22 service ready response and ... **Platforms**: win **CVEs**: CVE-2017-6416 **Refs**: source
SoftiaCom WMailserver 1.0 Buffer Overflow exploit/windows/smtp/wmailserver	2005-07-11	average	This module exploits a stack buffer overflo SoftiaCom WMailserver 1.0 (SMTP) via a S frame overwrite. **Platforms**: win **CVEs**: CVE-2005-2287 **Refs**: source
YPOPS 0.6 Buffer Overflow exploit/windows/smtp/ypops_overflow1	2004-09-27	average	This module exploits a stack buffer overflo the YPOPS POP3 service. This is a classic stack buffer overflow for YPOPS version 0. Possibly Affected version 0.5, 0.4.5.1, 0.4.5 point to jmp ... **Platforms**: win **CVEs**: CVE-2004-1558 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow exploit/windows/ssh/freeftpd_key_exchange	2006-05-12	average	This module exploits a simple stack buffer overflow in FreeFTPd 1.0.10 This flaw is du a buffer overflow error when handling a spe crafted key exchange algorithm string rece from an SSH ... **Platforms**: win **CVEs**: CVE-2006-2407 **Refs**: source
Freesshd Authentication Bypass exploit/windows/ssh/freesshd_authbypass	2010-08-11	excellent	This module exploits a vulnerability found i FreeSSHd <= 1.2.6 to bypass authenticatic You just need the username (which default root). The exploit has been tested with both password and ... **Platforms**: win **CVEs**: CVE-2012-6066 **Refs**: source, ref1, ref2
FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow exploit/windows/ssh/freesshd_key_exchange	2006-05-12	average	This module exploits a simple stack buffer overflow in FreeSSHd 1.0.9. This flaw is du a buffer overflow error when handling a spe crafted key exchange algorithm string rece from an SSH ... **Platforms**: win **CVEs**: CVE-2006-2407 **Refs**: source
PuTTY Buffer Overflow exploit/windows/ssh/putty_msg_debug	2002-12-16	normal	This module exploits a buffer overflow in th PuTTY SSH client that is triggered through validation error in SSH.c. This vulnerability affects versions 0.53 and earlier. **Platforms**: win **CVEs**: CVE-2002-1359 **Refs**: source, ref1
SecureCRT SSH1 Buffer Overflow exploit/windows/ssh/securecrt_ssh1	2002-07-23	average	This module exploits a buffer overflow in SecureCRT <= 4.0 Beta 2. By sending a vulnerable client an overly long SSH1 proto identifier string, it is possible to execute art code. This module ... **Platforms**: win **CVEs**: CVE-2002-1059 **Refs**: source
Sysax 5.53 SSH Username Buffer Overflow exploit/windows/ssh/sysax_ssh_username	2012-02-27	normal	This module exploits a vulnerability found i Sysax's SSH service. By supplying a long username, the SSH server will copy that da the stack without proper bounds checking, therefore allowing ... **Platforms**: win **Refs**: source, ref1
MS04-011 Microsoft Private Communications Transport Overflow exploit/windows/ssl/ms04_011_pct	2004-04-13	average	This module exploits a buffer overflow in th Microsoft Windows SSL PCT protocol stac This code is based on Johnny Cyberpunk's release and has been tested against Windo 2000 and Windows XP. ... **Platforms**: win **CVEs**: CVE-2003-0719 **Refs**: source
GAMSoft TelSrv 1.5 Username Buffer Overflow exploit/windows/telnet/gamsoft_telsrv_username	2000-07-17	average	This module exploits a username sprintf sta buffer overflow in GAMSoft TelSrv 1.5. Oth versions may also be affected. The service terminates after exploitation, so you only g one chance!. **Platforms**: win **CVEs**: CVE-2000-0665 **Refs**: source, ref1
GoodTech Telnet Server Buffer Overflow exploit/windows/telnet/goodtech_telnet	2005-03-15	average	This module exploits a stack buffer overflo GoodTech Systems Telnet Server versions to 5.0.7. By sending an overly long string, a attacker can overwrite the buffer and contr program ... **Platforms**: win **CVEs**: CVE-2005-0768 **Refs**: source

Metasploit Module	Date	Rank	Details
Allied Telesyn TFTP Server 1.9 Long Filename Overflow exploit/windows/tftp/attftp_long_filename	2006-11-27	average	This module exploits a stack buffer overflo AT-TFTP v1.9, by sending a request (get/w for an overly long file name. **Platforms**: win **CVEs**: CVE-2006-6184 **Refs**: source
Distinct TFTP 3.10 Writable Directory Traversal Execution exploit/windows/tftp/distinct_tftp_traversal	2012-04-08	excellent	This module exploits a directory traversal vulnerability in the TFTP Server componen Distinct Intranet Servers version 3.10 whicl allows a remote attacker to write arbitrary f to the server ... **Platforms**: win **CVEs**: CVE-2012-6664 **Refs**: source, ref1
D-Link TFTP 1.0 Long Filename Buffer Overflow exploit/windows/tftp/dlink_long_filename	2007-03-12	good	This module exploits a stack buffer overflo D-Link TFTP 1.0. By sending a request for overly long file name, an attacker could ov a buffer and execute arbitrary code. For be results, ... **Platforms**: win **CVEs**: CVE-2007-1435 **Refs**: source
FutureSoft TFTP Server 2000 Transfer-Mode Overflow exploit/windows/tftp/futuresoft_transfermode	2005-05-31	average	This module exploits a stack buffer overflo the FutureSoft TFTP Server 2000 product. sending an overly long transfer-mode strin were able to overwrite both the SEH and th saved EIP. A ... **Platforms**: win **CVEs**: CVE-2005-1812 **Refs**: source
NetDecision 4.2 TFTP Writable Directory Traversal Execution exploit/windows/tftp/netdecision_tftp_traversal	2009-05-16	excellent	This module exploits a vulnerability found i NetDecision 4.2 TFTP server. The software contains a directory traversal vulnerability t allows a remote attacker to write arbitrary f the file ... **Platforms**: win **CVEs**: CVE-2009-1730 **Refs**: source
OpenTFTP SP 1.4 Error Packet Overflow exploit/windows/tftp/opentftp_error_code	2008-07-05	average	This module exploits a buffer overflow in OpenTFTP Server SP 1.4. The vulnerable condition triggers when the TFTP opcode i configured as an error packet, the TFTP se will then format the ... **Platforms**: win **CVEs**: CVE-2008-2161 **Refs**: source, ref1
Quick FTP Pro 2.1 Transfer-Mode Overflow exploit/windows/tftp/quick_tftp_pro_mode	2008-03-27	good	This module exploits a stack buffer overflo the Quick TFTP Pro server product. MS Up KB926436 screws up the opcode address used in oledlg.dll resulting in a DoS. This is port of a ... **Platforms**: win **CVEs**: CVE-2008-1610 **Refs**: source, ref1
TFTPD32 Long Filename Buffer Overflow exploit/windows/tftp/tftpd32_long_filename	2002-11-19	average	This module exploits a stack buffer overflo TFTPD32 version 2.21 and prior. By sendir request for an overly long file name to the tftpd32 server, a remote attacker could ove a buffer and ... **Platforms**: win **CVEs**: CVE-2002-2226 **Refs**: source
TFTPDWIN v0.4.2 Long Filename Buffer Overflow exploit/windows/tftp/tftpdwin_long_filename	2006-09-21	great	This module exploits the ProSysInfo TFTP threaded TFTP Server. By sending an over long file name to the tftpd.exe server, the s can be overwritten. **Platforms**: win **CVEs**: CVE-2006-4948 **Refs**: source

Metasploit Module	Date	Rank	Details
TFTP Server for Windows 1.4 ST WRQ Buffer Overflow exploit/windows/tftp/tftpserver_wrq_bof	2008-03-26	normal	This module exploits a vulnerability found i TFTP Server 1.4 ST. The flaw is due to the TFTP handles the filename parameter extr from a WRQ request. The server will appe the user-supplied ... **Platforms**: win **CVEs**: CVE-2008-1611 **Refs**: source
3CTftpSvc TFTP Long Mode Buffer Overflow exploit/windows/tftp/threectftpsvc_long_mode	2006-11-27	great	This module exploits a stack buffer overflo 3CTftpSvc 2.0.1. By sending a specially cr packet with an overly long mode field, a re attacker could overflow a buffer and execu arbitrary ... **Platforms**: win **CVEs**: CVE-2006-6183 **Refs**: source, ref1
CA CAM log_security() Stack Buffer Overflow (Win32) exploit/windows/unicenter/cam_log_security	2005-08-22	great	This module exploits a vulnerability in the C CAM service by passing a long parameter log_security() function. The CAM service is of TNG Unicenter. This module has been t on ... **Platforms**: win **CVEs**: CVE-2005-2668 **Refs**: source
RealVNC 3.3.7 Client Buffer Overflow exploit/windows/vnc/realvnc_client	2001-01-29	normal	This module exploits a buffer overflow in RealVNC 3.3.7 (vncviewer.exe). **Platforms**: win **CVEs**: CVE-2001-0167 **Refs**: source
UltraVNC 1.0.1 Client Buffer Overflow exploit/windows/vnc/ultravnc_client	2006-04-04	normal	This module exploits a buffer overflow in UltraVNC Win32 Viewer 1.0.1 Release. **Platforms**: win **CVEs**: CVE-2006-1652 **Refs**: source
UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow exploit/windows/vnc/ultravnc_viewer_bof	2008-02-06	normal	This module exploits a buffer overflow in UltraVNC Viewer 1.0.2 Release. If a malici server responds to a client connection indi a minor protocol version of 14 or 16, a 32-b integer is ... **Platforms**: win **CVEs**: CVE-2008-0610 **Refs**: source
WinVNC Web Server GET Overflow exploit/windows/vnc/winvnc_http_get	2001-01-29	average	This module exploits a buffer overflow in th AT&T WinVNC version <= v3.3.3r7 web se When debugging mode with logging is ena (non-default), an overly long GET request overwrite the ... **Platforms**: win **CVEs**: CVE-2001-0168 **Refs**: source
SafeNet SoftRemote IKE Service Buffer Overflow exploit/windows/vpn/safenet_ike_11	2009-06-01	average	This module exploits a stack buffer overflo Safenet SoftRemote IKE IreIKE.exe servic When sending a specially crafted udp pack port 62514 an attacker may be able to exe arbitrary code. ... **Platforms**: win **CVEs**: CVE-2009-1943 **Refs**: source, ref1
WinRM Script Exec Remote Code Execution exploit/windows/winrm/winrm_script_exec	2012-11-01	manual	This module uses valid credentials to login the WinRM service and execute a payload has two available methods for payload deli Powershell 2.0 and VBS CmdStager. The module will check if ... **Platforms**: win **Refs**: source, ref1
MS04-045 Microsoft WINS Service Memory Overwrite exploit/windows/wins/ms04_045_wins	2004-12-14	great	This module exploits an arbitrary memory v flaw in the WINS service. This exploit has b tested against Windows 2000 only. **Platforms**: win **CVEs**: CVE-2004-1080 **Refs**: source

Showing 1 to 1,325 of 1,325 entries

How to find exploits in Metasploit

Beside the above table, here's how you can find exploits via the Metasploit console (msfconsole).

List all exploits:

```
msf6 > search type:exploit
```

Search exploits by CVE:

```
msf6 > search type:exploit cve:2021
```

Find exploits by OS (platform):

```
msf6 > search type:exploit platform:windows
```

Find exploits by OS (target):

```
msf6 > search type:exploit target:windows
```

Search exploits by name:

```
msf6 > search type:exploit eternalblue
```

Find exploits by port:

```
msf6 > search type:exploit port:445
```

You can also combine those parameters to narrow down your search results.

Note that the presented table above will likely provide more exploit candidates for the same equivalent searches, because the data has been collected from the full module descriptions and by analyzing the exploit source codes as well, not just what is the officially listed supported platform or target.

Therefore, it should be the most comprehensive list of Metasploit Windows exploits available.

If you find this list useful, please consider subscribing and following InfosecMatter on Twitter, Facebook or Github to keep up with the latest developments. You can also support this website through a donation.

See also

- Metasploit Auxiliary Modules (Detailed Spreadsheet)
- Metasploit Linux Exploits (Detailed Spreadsheet)
- Post Exploitation Metasploit Modules (Reference)
- Metasploit Payloads (Detailed Spreadsheet)
- Metasploit Android Modules
- Metasploit Module Library

SHARE THIS

TAGS | Cheatsheet | CVE | Denial-of-service | EternalBlue | Exploitation | Metasploit | Msfconsole | Privilege escalation | ProxyLogon | RCE | SharePoint | Spreadsheet | Windows