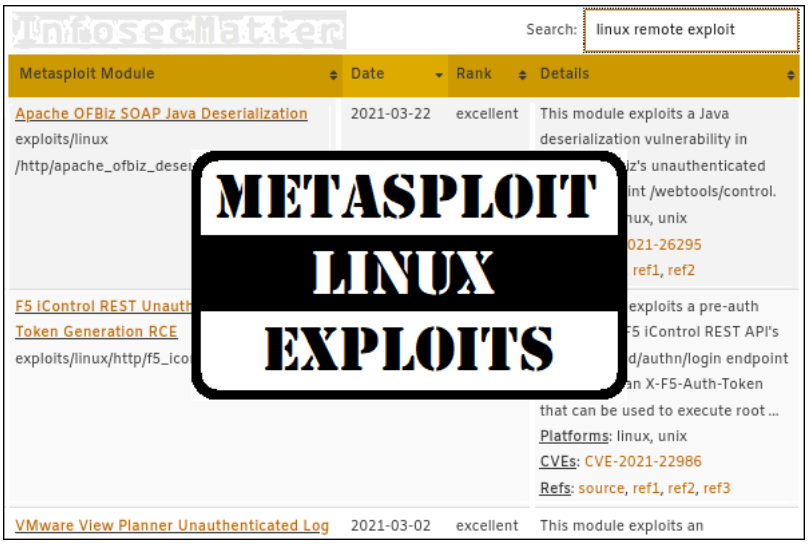
List of Metasploit Linux Exploits (Detailed Spreadsheet)

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

April 14, 2021



On this page you will find a comprehensive list of all **Metasploit Linux 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 573 of them which are either:

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

Thus, this list should contain all Metasploit exploits that can be used against Linux 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: **`vmware rce`**
  Display only remote code execution exploits for VMware products.
- Search for: **`cve-2021`**
  Display only exploits with assigned CVE from year 2021.
- Search for **`auth bypass`**
  Display only authentication bypass exploits.
- Search for **`privilege escalation kernel`**
  Display only Linux kernel privilege escalation exploits.
- Search for: **`shellshock`**
  Display only modules exploiting the Shellshock vulnerability (CVE-2014-6271).

Alright, now let's get to the list.

List of Metasploit Linux exploits

Metasploit Module	Date	Rank	Details
Android ADB Debug Server Remote Payload Execution exploit/android/adb/adb_server_exec	2016-01-01	excellent	Writes and spawns a native pa android device that is listening messages. **Platforms**: linux **Refs**: source
Android Stagefright MP4 tx3g Integer Overflow exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	This module exploits an integer vulnerability in the Stagefright L (libstagefright.so). The vulnerat parsing specially crafted MP4 f variety of ... **Platforms**: linux **CVEs**: CVE-2015-3864 **Refs**: source, ref1, ref2, ref3, re ref7
Android Browser and WebView addJavascriptInterface Code Execution exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	This module exploits a privilege in Android < 4.2's WebView cor arises when untrusted Javascri executed by a WebView that ha Interfaces added to it. ... **Platforms**: android, linux **CVEs**: CVE-2012-6636, CVE-2 **Refs**: source, ref1, ref2, ref3, re
Android Binder Use-After-Free Exploit exploit/android/local/binder_uaf	2019-09-26	excellent	This module exploits CVE-2019 a use-after-free in Binder in the The bug is a local privilege esc vulnerability that allows for a fu a vulnerable ... **Platforms**: android, linux **CVEs**: CVE-2019-2215 **Refs**: source, ref1, ref2, ref3, re
Android 'Towelroot' Futex Requeue Kernel Exploit exploit/android/local/futex_requeue	2014-05-03	excellent	This module exploits a bug in fu the Linux kernel, using similar t employed by the towelroot expl device with a kernel built before likely to be ... **Platforms**: android, linux **CVEs**: CVE-2014-3153 **Refs**: source, ref1, ref2
Android get_user/put_user Exploit exploit/android/local/put_user_vroot	2013-09-06	excellent	This module exploits a missing get_user and put_user API fun kernel before 3.5.5. The missin these functions allow an unpriv read and write ... **CVEs**: CVE-2013-6282 **Refs**: source, ref1, ref2, ref3
Android 'su' Privilege Escalation exploit/android/local/su_exec	2017-08-31	manual	This module uses the su binary rooted devices to run a payloac rooted Android device will conta (often linked with an applicatior user to run ... **Platforms**: android, linux **Refs**: source
Firefox Exec Shellcode from Privileged Javascript Shell exploit/firefox/local/exec_shellcode	2014-03-10	excellent	This module allows execution c from a privileged Firefox Javas places the specified payload in the necessary protection flags, which can ... **Platforms**: firefox, linux, osx, u **Refs**: source
eScan Web Management Console Command Injection exploit/linux/antivirus/escan_password_exec	2014-04-04	excellent	This module exploits a comma vulnerability found in the eScar Management Console. The vul while processing CheckPass lo attacker with a valid username **Platforms**: linux **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Adobe Flash Player ActionScript Launch Command Execution Vulnerability exploit/linux/browser/adobe_flashplayer_aslaunch	2008-12-17	good	This module exploits a vulnerat Flash Player for Linux, version 9.0.151.0 and prior. An input va vulnerability allows command e the browser loads a ... **Platforms**: unix **CVEs**: CVE-2008-5499 **Refs**: source, ref1
ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux) exploit/linux/ftp/proftp_sreplace	2006-11-26	great	This module exploits a stack-ba overflow in versions 1.2 throug ProFTPD server. The vulnerabi "sreplace" function within the "s The off-by-one ... **Platforms**: linux **CVEs**: CVE-2006-5815 **Refs**: source, ref1, ref2, ref3, re
ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux) exploit/linux/ftp/proftp_telnet_iac	2010-11-01	great	This module exploits a stack-ba overflow in versions of ProFTP between versions 1.3.2rc3 and sending data containing a large Telnet IAC commands, an attac **Platforms**: linux **CVEs**: CVE-2010-4221 **Refs**: source
Unreal Tournament 2004 "secure" Overflow (Linux) exploit/linux/games/ut2004_secure	2004-06-18	good	This is an exploit for the Game in the Unreal Engine. This expl one UDP packet, which can be and sent to a broadcast addres GameSpy query ... **Platforms**: linux **CVEs**: CVE-2004-0608 **Refs**: source
Accellion FTA getStatus verify_oauth_token Command Execution exploit/linux/http/accellion_fta_getstatus_oauth	2015-07-10	excellent	This module exploits a metacha injection vulnerability in the Acc Transfer appliance. This vulner triggered when a user-provided passed into a ... **Platforms**: unix **CVEs**: CVE-2015-2857 **Refs**: source, ref1
Advantech Switch Bash Environment Variable Code Injection (Shellshock) exploit/linux/http/advantech_switch_bash_env_exec	2015-12-01	excellent	This module exploits the Shells vulnerability, a flaw in how the B handles external environment v module targets the 'ping.sh' CG accessible through the Boa we **Platforms**: unix **CVEs**: CVE-2014-6271 **Refs**: source, ref1, ref2, ref3
Airties login-cgi Buffer Overflow exploit/linux/http/airties_login_cgi_bof	2015-03-31	normal	This module exploits a remote vulnerability on several Airties r vulnerability exists in the handli queries to the login cgi with lon parameters. The ... **Platforms**: linux **CVEs**: CVE-2015-2797 **Refs**: source, ref1
Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution exploit/linux/http/alcatel_omnipcx_mastercgi_exec	2007-09-09	manual	This module abuses a metacha vulnerability in the HTTP mana of the Alcatel-Lucent OmniPCX Communication Server 7.1 and Unified Maintenance Tool ... **Platforms**: unix **CVEs**: CVE-2007-3010 **Refs**: source, ref1
AlienVault OSSIM/USM Remote Code Execution exploit/linux/http/alienvault_exec	2017-01-31	excellent	This module exploits object inje authentication bypass and ip sp vulnerabilities all together. Una users can execute arbitrary cor the context of the root user. By **Platforms**: python **CVEs**: CVE-2016-8582 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
AlienVault OSSIM SQL Injection and Remote Code Execution exploit/linux/http/alienvault_sqli_exec	2014-04-24	excellent	This module exploits an unauth injection vulnerability affecting A OSSIM versions 4.3.1 and lowe injection issue can be abused i retrieve an active admin ... **Platforms**: unix **CVEs**: CVE-2016-8581 **Refs**: source
Apache Continuum Arbitrary Command Execution exploit/linux/http/apache_continuum_cmd_exec	2016-04-06	excellent	This module exploits a commar Apache Continuum <= 1.4.2. B command into the installation.v parameter to /continuum/savelr a shell can be ... **Platforms**: linux **Refs**: source
Apache CouchDB Arbitrary Command Execution exploit/linux/http/apache_couchdb_cmd_exec	2016-04-06	excellent	CouchDB administrative users database server via HTTP(S). S configuration options include pa system-level binaries that are s launched by ... **Platforms**: linux **CVEs**: CVE-2017-12635, CVE- **Refs**: source, ref1, ref2, ref3
Apache OFBiz XML-RPC Java Deserialization exploit/linux/http/apache_ofbiz_deserialization	2020-07-13	excellent	This module exploits a Java de vulnerability in Apache OFBiz's XML-RPC endpoint /webtools/c versions prior to 17.12.04. **Platforms**: linux, unix **CVEs**: CVE-2020-9496 **Refs**: source, ref1, ref2, ref3
Apache OFBiz SOAP Java Deserialization exploit/linux/http/apache_ofbiz_deserialization_soap	2021-03-22	excellent	This module exploits a Java de vulnerability in Apache OFBiz's SOAP endpoint /webtools/contr for versions prior to 17.12.06. **Platforms**: linux, unix **CVEs**: CVE-2021-26295 **Refs**: source, ref1, ref2
Artica proxy 4.30.000000 Auth Bypass service-cmds-peform Command Injection exploit/linux/http/artica_proxy_auth_bypass_service_cmds_peform_command_injection	2020-08-09	excellent	This module exploits an authen command injection vulnerability combined with an authenticatio discovered on the same versio trigger the ... **Platforms**: linux, unix **CVEs**: CVE-2020-17505, CVE- **Refs**: source, ref1
Astium Remote Code Execution exploit/linux/http/astium_sqli_upload	2013-09-17	manual	This module exploits vulnerabil Astium astium-confweb-2.1-25 lower. A SQL Injection vulnerab achieve authentication bypass access. From an ... **Platforms**: php **Refs**: source
AsusWRT LAN Unauthenticated Remote Code Execution exploit/linux/http/asuswrt_lan_rce	2018-01-22	excellent	The HTTP server in AsusWRT it allows an unauthenticated cli POST in certain cases. This ca with another vulnerability in the configuration upload ... **Platforms**: unix **CVEs**: CVE-2018-5999, CVE-2 **Refs**: source, ref1, ref2, ref3
ATutor 2.2.1 Directory Traversal / Remote Code Execution exploit/linux/http/atutor_filemanager_traversal	2016-03-01	excellent	This module exploits a directory vulnerability in ATutor on an Ap with display_errors set to On, w used to allow us to upload a ma On the web ... **Platforms**: php **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
Belkin Play N750 login.cgi Buffer Overflow exploit/linux/http/belkin_login_bof	2014-05-09	normal	This module exploits a remote vulnerability on Belkin Play N75 Dual-Band N+ Router N750 rou vulnerability exists in the handli queries with long 'jump' ... **Platforms**: linux **CVEs**: CVE-2014-1635 **Refs**: source, ref1, ref2
Bludit Directory Traversal Image File Upload Vulnerability exploit/linux/http/bludit_upload_images_exec	-	excellent	This module exploits a vulneral remote user could abuse the u the image upload feature in ord malicious payload anywhere or and then use a ... **Platforms**: php **CVEs**: CVE-2019-16113 **Refs**: source, ref1, ref2
Cayin CMS NTP Server RCE exploit/linux/http/cayin_cms_ntp	2020-06-04	excellent	This module exploits an authen Cayin CMS <= 11.0. The RCE system_service.cgi file's ntpIp F field is limited in size, so repeat made to ... **Platforms**: linux **CVEs**: CVE-2020-7357 **Refs**: source, ref1
Centreon Poller Authenticated Remote Command Execution exploit/linux/http/centreon_pollers_auth_rce	2020-01-27	excellent	An authenticated user with suff administrative rights to manage this functionality to execute arb remotely. Usually, the miscellar are used by the ... **Platforms**: linux, unix **Refs**: source
Centreon SQL and Command Injection exploit/linux/http/centreon_sqli_exec	2014-10-15	excellent	This module exploits several vu Centreon 2.5.1 and prior and C Enterprise Server 2.2 and prior combination of SQL injection a injection in the ... **Platforms**: unix **CVEs**: CVE-2014-3828, CVE-2 **Refs**: source, ref1
Centreon Web Useralias Command Execution exploit/linux/http/centreon_useralias_exec	2016-02-26	excellent	Centreon Web Interface <= 2.5 ECHO for logging SQL errors. T can be abused for arbitrary cod can be triggered via the login s **Platforms**: python **Refs**: source
Red Hat CloudForms Management Engine 5.1 agent/linuxpkgs Path Traversal exploit/linux/http/cfme_manageiq_evm_upload_exec	2013-09-04	excellent	This module exploits a path tra vulnerability in the "linuxpkgs" a controller of the Red Hat Cloud Management Engine 5.1 (Mana Virtualization Manager 5.0 and **Platforms**: ruby **CVEs**: CVE-2013-2068 **Refs**: source, ref1
Cisco Firepower Management Console 6.0 Post Authentication UserAdd Vulnerability exploit/linux/http/cisco_firepower_useradd	2016-10-10	excellent	This module exploits a vulneral Cisco Firepower Management management system contains a flaw that allows the www user t useradd binary, which can ... **Platforms**: linux **CVEs**: CVE-2016-6433 **Refs**: source, ref1
Cisco Prime Infrastructure Unauthenticated Remote Code Execution exploit/linux/http/cisco_prime_inf_rce	2018-10-04	excellent	Cisco Prime Infrastructure (CP basic flaws that when exploited unauthenticated attacker to ach code execution. The first flaw is vulnerability that ... **Platforms**: linux **CVEs**: CVE-2018-15379 **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
Cisco RV320 and RV325 Unauthenticated Remote Code Execution exploit/linux/http/cisco_rv32x_rce	2018-09-09	normal	This exploit module combines a disclosure (CVE-2019-1653) ar injection vulnerability (CVE-201 to gain unauthenticated remote on Cisco RV320 and ... **Platforms**: linux **CVEs**: CVE-2019-1652, CVE-2 **Refs**: source, ref1, ref2
Cisco UCS Director Cloupia Script RCE exploit/linux/http/cisco_ucs_cloupia_script_rce	2020-04-15	excellent	This module exploits an authen and directory traversals in Cisc 6.7.4.0 to leak the administrato and execute a Cloupia script cc arbitrary ... **Platforms**: linux, unix **CVEs**: CVE-2020-3243, CVE-2 **Refs**: source, ref1, ref2
Cisco UCS Director Unauthenticated Remote Code Execution exploit/linux/http/cisco_ucs_rce	2019-08-21	excellent	The Cisco UCS Director virtual contains two flaws that can be abused by an attacker to achie execution as root. The first one 1937, is an authentication ... **Platforms**: unix **CVEs**: CVE-2019-1936, CVE-2 **Refs**: source, ref1, ref2, ref3
Citrix ADC (NetScaler) Directory Traversal RCE exploit/linux/http/citrix_dir_traversal_rce	2019-12-17	excellent	This module exploits a directory Citrix Application Delivery Cont NetScaler, and Gateway 10.5, and 13.0, to execute an arbitrar payload. **Platforms**: python, unix **CVEs**: CVE-2019-19781 **Refs**: source, ref1, ref2, ref3
Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability exploit/linux/http/cpi_tararchive_upload	2019-05-15	excellent	This module exploits a vulnerab Cisco Prime Infrastructure. The TarArchive Java class the HA H component uses does not chec directory traversals ... **Platforms**: linux **CVEs**: CVE-2019-1821 **Refs**: source, ref1, ref2, ref3, re
Cisco RV110W/RV130(W)/RV215W Routers Management Interface Remote Command Execution exploit/linux/http/cve_2019_1663_cisco_rmi_rce	2019-02-27	good	A vulnerability in the web-based interface of the Cisco RV110W Firewall, Cisco RV130W Wirele Multifunction VPN Router, and Wireless-N VPN Router could a **Platforms**: linux **CVEs**: CVE-2019-1663 **Refs**: source, ref1, ref2
DC/OS Marathon UI Docker Exploit exploit/linux/http/dcos_marathon	2017-03-03	excellent	Utilizing the DCOS Cluster's Ma attacker can create a docker cc '/' path mounted with read/write the host server that is running t container. As ... **Platforms**: python **Refs**: source, ref1
DD-WRT HTTP Daemon Arbitrary Command Execution exploit/linux/http/ddwrt_cgibin_exec	2009-07-20	excellent	This module abuses a metacha vulnerability in the HTTP mana wireless gateways running DD- allows an unauthenticated attac arbitrary ... **Platforms**: unix **CVEs**: CVE-2009-2765 **Refs**: source
DenyAll Web Application Firewall Remote Code Execution exploit/linux/http/denyall_waf_exec	2017-09-19	excellent	This module exploits the comm vulnerability of DenyAll Web Ap Firewall. Unauthenticated users terminal command under the cc server user. **Platforms**: python **CVEs**: CVE-2017-14706 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
D-Link authentication.cgi Buffer Overflow exploit/linux/http/dlink_authentication_cgi_bof	2013-02-08	normal	This module exploits a remote vulnerability on several D-Link vulnerability exists in the handli queries to the authentication.cg password values. ... **Platforms**: linux **Refs**: source, ref1, ref2, ref3
D-Link Devices Unauthenticated Remote Command Execution exploit/linux/http/dlink_command_php_exec_noauth	2013-02-04	excellent	Various D-Link Routers are vuln command injection via the web vulnerability exists in command accessible without authenticati has been tested ... **Platforms**: unix **Refs**: source, ref1, ref2, ref3
D-Link DCS-931L File Upload exploit/linux/http/dlink_dcs931l_upload	2015-02-23	great	This module exploits a file uplo D-Link DCS-931L network cam setFileUpload functionality allo users to upload files to anywhe system, ... **Platforms**: linux **CVEs**: CVE-2015-2049 **Refs**: source, ref1, ref2
D-Link DCS-930L Authenticated Remote Command Execution exploit/linux/http/dlink_dcs_930l_authenticated_remote_command_execution	2015-12-20	excellent	The D-Link DCS-930L Network vulnerable to OS Command Inj web interface. The vulnerability /setSystemCommand, which is credentials. This ... **Platforms**: unix **Refs**: source
D-Link DIR-645 / DIR-815 diagnostic.php Command Execution exploit/linux/http/dlink_diagnostic_exec_noauth	2013-03-05	excellent	Some D-Link Routers are vulne Command injection in the web DIR-645 versions prior 1.03 aut needed to exploit it. On version authentication is needed in ... **Platforms**: linux, unix **CVEs**: CVE-2014-100005 **Refs**: source, ref1
D-Link Devices Unauthenticated Remote Command Execution exploit/linux/http/dlink_dir300_exec_telnet	2013-04-22	excellent	Various D-Link Routers are vuln command injection via the web vulnerability exists in tools_vct. accessible with credentials. Acc vulnerability ... **Platforms**: unix **Refs**: source, ref1
D-Link DIR-605L Captcha Handling Buffer Overflow exploit/linux/http/dlink_dir605l_captcha_bof	2012-10-08	manual	This module exploits an anonyn code execution vulnerability on routers. The vulnerability exists user supplied captcha informat the insecure ... **Platforms**: linux **Refs**: source, ref1
D-Link DIR615h OS Command Injection exploit/linux/http/dlink_dir615_up_exec	2013-02-07	excellent	Some D-Link Routers are vulne authenticated OS command inj web interface, where default cr admin/admin or admin/passwo blind os command ... **Platforms**: linux, unix **Refs**: source, ref1
DIR-850L (Un)authenticated OS Command Exec exploit/linux/http/dlink_dir850l_unauth_exec	2017-08-09	excellent	This module leverages an unau credential disclosure vulnerabil execute arbitrary commands or routers as an authenticated use Meterpreter payloads. **Platforms**: linux **Refs**: source, ref1, ref2
D-Link DSL-2750B OS Command Injection exploit/linux/http/dlink_dsl2750b_exec_noauth	2016-02-05	great	This module exploits a remote injection vulnerability in D-Link devices. Vulnerability can be ex "cli" parameter that is directly u "ayecli" binary. ... **Platforms**: linux **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
D-Link info.cgi POST Request Buffer Overflow exploit/linux/http/dlink_dspw215_info_cgi_bof	2014-05-22	normal	This module exploits an anonyr code execution vulnerability on devices. The vulnerability is a s buffer overflow in the my_cgi.cg when handling ... **Platforms**: linux **Refs**: source, ref1
DLINK DWL-2600 Authenticated Remote Command Injection exploit/linux/http/dlink_dwl_2600_command_injection	2019-05-15	excellent	Some DLINK Access Points ar an authenticated OS command Default credentials for the web admin/admin. **Platforms**: linux, unix **CVEs**: CVE-2019-20499 **Refs**: source
D-Link hedwig.cgi Buffer Overflow in Cookie Header exploit/linux/http/dlink_hedwig_cgi_bof	2013-02-08	normal	This module exploits an anonyr code execution vulnerability on routers. The vulnerability exists of HTTP queries to the hedwig. value cookies. ... **Platforms**: linux **Refs**: source, ref1, ref2, ref3
D-Link HNAP Request Remote Buffer Overflow exploit/linux/http/dlink_hnap_bof	2014-05-15	normal	This module exploits an anonyr code execution vulnerability on devices. The vulnerability is du based buffer overflow while har HTTP POST ... **Platforms**: linux **CVEs**: CVE-2014-3936 **Refs**: source, ref1, ref2
D-Link Devices HNAP SOAPAction-Header Command Execution exploit/linux/http/dlink_hnap_header_exec_noauth	2015-02-13	normal	Different D-Link Routers are vu command injection in the HNAI interface. Since it is a blind OS injection vulnerability, there is n executed command. This ... **Platforms**: linux **Refs**: source, ref1, ref2
Dlink DIR Routers Unauthenticated HNAP Login Stack Buffer Overflow exploit/linux/http/dlink_hnap_login_bof	2016-11-07	excellent	Several Dlink routers contain a authentication stack buffer over which is exposed on the LAN ir 80. This vulnerability affects the protocol, which ... **Platforms**: linux **CVEs**: CVE-2016-6563 **Refs**: source, ref1, ref2
D-Link Devices UPnP SOAP Command Execution exploit/linux/http/dlink_upnp_exec_noauth	2013-07-05	normal	Different D-Link Routers are vu command injection in the UPnP Since it is a blind OS commanc vulnerability, there is no output command. This ... **Platforms**: linux **CVEs**: CVE-2014-8361 **Refs**: source, ref1
dnaLIMS Admin Module Command Execution exploit/linux/http/dnalims_admin_exec	2017-03-08	excellent	This module utilizes an adminis which allows for command exe is completely unprotected from authentication when given a PC **Platforms**: linux, unix **CVEs**: CVE-2017-6526 **Refs**: source, ref1
Docker Daemon - Unprotected TCP Socket Exploit exploit/linux/http/docker_daemon_tcp	2017-07-25	excellent	Utilizing Docker via unprotected (2375/tcp, maybe 2376/tcp with tls-auth), an attacker can create container with the '/' path moun read/write permissions ... **Platforms**: linux, python **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Dolibarr ERP/CRM Post-Auth OS Command Injection exploit/linux/http/dolibarr_cmd_exec	2012-04-06	excellent	This module exploits a vulnerat Dolibarr ERP/CRM 3's backup software is used to manage a c business information such as c orders, stocks, agenda, ... **Platforms**: linux, unix **Refs**: source, ref1
OpenPLI Webif Arbitrary Command Execution exploit/linux/http/dreambox_openpli_shell	2013-02-08	great	Some Dream Boxes with Open Images are vulnerable to OS c in the Webif 6.0.4 Web Interfac injection, which means that you output of your ... **Platforms**: linux, unix **Refs**: source, ref1, ref2
Endian Firewall Proxy Password Change Command Injection exploit/linux/http/efw_chpasswd_exec	2015-06-28	excellent	This module exploits an OS co vulnerability in a web-accessibl used to change passwords for proxy user accounts. Valid crec an account are ... **Platforms**: linux **CVEs**: CVE-2015-5082 **Refs**: source, ref1
PowerShellEmpire Arbitrary File Upload (Skywalker) exploit/linux/http/empire_skywalker	2016-10-15	excellent	A vulnerability existed in the Pc server prior to commit f030cf62 allow an arbitrary file to be writt controlled location with the perr Empire ... **Platforms**: linux, python **Refs**: source, ref1
E-Mail Security Virtual Appliance learn-msg.cgi Command Injection exploit/linux/http/esva_exec	2012-08-16	excellent	This module exploits a comma vulnerability found in E-Mail Se Appliance. This module abuses msg.cgi file to execute arbitrary without authentication. ... **Platforms**: unix **Refs**: source
EyesOfNetwork 5.1-5.3 AutoDiscovery Target Command Execution exploit/linux/http/eyesofnetwork_autodiscovery_rce	2020-02-06	excellent	This module exploits multiple v EyesOfNetwork version 5.1, 5.2 to execute arbitrary commands module takes advantage of a c injection ... **Platforms**: linux, unix **CVEs**: CVE-2020-8654, CVE-2 2020-8656, CVE-2020-8657, C **Refs**: source
Axis Network Camera .srv to parhand RCE exploit/linux/http/axis_srv_parhand_rce	2018-06-18	excellent	This module exploits an auth by functionality and a command in parhand to execute code as the **Platforms**: linux, unix **CVEs**: CVE-2018-10660, CVE- CVE-2018-10662 **Refs**: source, ref1, ref2
Crypttech CryptoLog Remote Code Execution exploit/linux/http/crypttech_cryptolog_login_exec	2017-05-03	excellent	This module exploits a SQL inje command injection vulnerability version of CryptoLog. An unaut can execute a terminal comma context of the web user. ... **Platforms**: python **Refs**: source, ref1
D-Link Cookie Command Execution exploit/linux/http/dlink_dspw110_cookie_noauth_exec	2015-06-12	normal	This module exploits an anonyr upload and code execution vuln different D-Link devices. The vu command injection in the cooki process of the lighttpd ... **Platforms**: linux **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
F5 BIG-IP TMUI Directory Traversal and File Upload RCE exploit/linux/http/f5_bigip_tmui_rce	2020-06-30	average	This module exploits a directory BIG-IP Traffic Management Us (TMUI) to upload a shell script the Unix root user. Unix shell a by ... **Platforms**: linux, unix **CVEs**: CVE-2020-5902 **Refs**: source, ref1, ref2
HP VAN SDN Controller Root Command Injection exploit/linux/http/hp_van_sdn_cmd_inject	2018-06-25	excellent	This module exploits a hardcod or default credentials in HPE V/ Controller <= 2.7.18.0503 to ex as root. A root command injecti discovered in the uninstall ... **Platforms**: linux, unix **Refs**: source, ref1
LifeSize UVC Authenticated RCE via Ping exploit/linux/http/lifesize_uvc_ping_rce	2014-03-21	excellent	When authenticated as an adm LifeSize UVC 1.2.6, an attacke ping diagnostic functionality to command execution as the ww equivalent). **Platforms**: unix **Refs**: source
Mutiny 5 Arbitrary File Upload exploit/linux/http/mutiny_frontend_upload	2013-05-15	excellent	This module exploits a code ex the Mutiny 5 appliance. The Ed servlet provides a file upload fu authenticated users. A directory vulnerability in the same ... **Platforms**: linux **CVEs**: CVE-2013-0136 **Refs**: source, ref1
Nexus Repository Manager Java EL Injection RCE exploit/linux/http/nexus_repo_manager_el_injection	2020-03-31	excellent	This module exploits a Java Ex Language (EL) injection in Nex Manager versions up to and inc execute code as the Nexus use authentication ... **Platforms**: linux **CVEs**: CVE-2020-10199 **Refs**: source, ref1, ref2
PineApp Mail-SeCure ldapsyncnow.php Arbitrary Command Execution exploit/linux/http/pineapp_ldapsyncnow_exec	2013-07-26	excellent	This module exploits a commar vulnerability on PineApp Mail-S vulnerability exists on the ldaps component, due to the insecure shell_exec() php ... **Platforms**: unix **Refs**: source
Samsung SRN-1670D Web Viewer Version 1.0.0.193 Arbitrary File Read and Upload exploit/linux/http/samsung_srv_1670d_upload_exec	2017-03-14	good	This module exploits an unrestı vulnerability in Web Viewer 1.0 Samsung SRN-1670D devices network_ssl_upload.php file all authenticated attackers to uplo **Platforms**: php **CVEs**: CVE-2015-8279, CVE-2 **Refs**: source, ref1, ref2
Tiki-Wiki CMS Calendar Command Execution exploit/linux/http/tiki_calendar_exec	2016-06-06	excellent	Tiki-Wiki CMS's calendar modu remote code execution vulnera viewmode GET parameter. The module is NOT enabled by defa the default permissions ... **Platforms**: php **Refs**: source, ref1
V-CMS PHP File Upload and Execute exploit/linux/http/vcms_upload	2011-11-27	excellent	This module exploits a vulnerat CMS's inline image upload feat is due to the inline_image_uplo checking the file type before sa web ... **Platforms**: linux, php **CVEs**: CVE-2011-4828 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
F5 iControl iCall::Script Root Command Execution exploit/linux/http/f5_icall_cmd	2015-09-03	excellent	This module exploits an authen escalation vulnerability in the iC the F5 BIG-IP LTM (and likely c This requires valid credentials a ... **Platforms**: unix **CVEs**: CVE-2015-3628 **Refs**: source, ref1, ref2
F5 iControl Remote Root Command Execution exploit/linux/http/f5_icontrol_exec	2013-09-17	excellent	This module exploits an authen command execution vulnerabili BIGIP iControl API (and likely c **Platforms**: unix **CVEs**: CVE-2014-2928 **Refs**: source, ref1
F5 iControl REST Unauthenticated SSRF Token Generation RCE exploit/linux/http/f5_icontrol_rest_ssrf_rce	2021-03-10	excellent	This module exploits a pre-auth iControl REST API's /mgmt/sha endpoint to generate an X-F5-A can be used to execute root co affected BIG-IP or ... **Platforms**: linux, unix **CVEs**: CVE-2021-22986 **Refs**: source, ref1, ref2, ref3
Foreman (Red Hat OpenStack/Satellite) bookmarks/create Code Injection exploit/linux/http/foreman_openstack_satellite_code_exec	2013-06-06	excellent	This module exploits a code inj vulnerability in the 'create' actio controller of Foreman and Red OpenStack/Satellite (Foreman earlier). **Platforms**: ruby **CVEs**: CVE-2013-2121 **Refs**: source, ref1, ref2
Fritz!Box Webcm Unauthenticated Command Injection exploit/linux/http/fritzbox_echo_exec	2014-02-11	excellent	Different Fritz!Box devices are unauthenticated OS command module was tested on a Fritz!B LAN side. The vendor reported devices ... **Platforms**: linux **CVEs**: CVE-2014-9727 **Refs**: source, ref1, ref2, ref3, re
Geutebruck testaction.cgi Remote Command Execution exploit/linux/http/geutebruck_testaction_exec	2020-05-20	excellent	This module exploits an authen command execution vulnerabili 'server' GET parameter of the / cgi/testaction.cgi page of Geute EEC-2xxx and G-Code ... **Platforms**: linux, unix **CVEs**: CVE-2020-16205 **Refs**: source, ref1, ref2, ref3
Github Enterprise Default Session Secret And Deserialization Vulnerability exploit/linux/http/github_enterprise_secret	2017-03-15	excellent	This module exploits two secur Github Enterprise, version 2.8.(is that the session managemen coded secret value, which can sign a serialized ... **Platforms**: linux **Refs**: source, ref1, ref2
Gitlist Unauthenticated Remote Command Execution exploit/linux/http/gitlist_exec	2014-06-30	excellent	This module exploits an unauth command execution vulnerabili 0.4.0 of Gitlist. The problem ex handling of a specially crafted f trying to blame it. **Platforms**: unix **CVEs**: CVE-2014-4511 **Refs**: source, ref1
GoAhead Web Server LD_PRELOAD Arbitrary Module Load exploit/linux/http/goahead_ldpreload	2017-12-18	excellent	This module triggers an arbitrar load vulnerability in GoAhead v versions between 2.5 and that module enabled. **Platforms**: linux, unix **CVEs**: CVE-2017-17562 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
GoAutoDial 3.3 Authentication Bypass / Command Injection exploit/linux/http/goautodial_3_rce_command_injection	2015-04-21	excellent	This module exploits a SQL inj login functionality for GoAutoDi 1406088000 and below, and at perform command injection. Th to retrieve the ... **Platforms**: linux **CVEs**: CVE-2015-2843, CVE-2 **Refs**: source
Berlios GPSD Format String Vulnerability exploit/linux/http/gpsd_format_string	2005-05-25	average	This module exploits a format s in the Berlios GPSD server. Th was discovered by Kevin Finist **Platforms**: linux **CVEs**: CVE-2004-1388 **Refs**: source, ref1
GroundWork monarch_scan.cgi OS Command Injection exploit/linux/http/groundwork_monarch_cmd_exec	2013-03-08	excellent	This module exploits a vulnerat GroundWork 6.7.0. This softwa network, application and cloud vulnerability exists in the mona where user ... **Platforms**: linux, unix **CVEs**: CVE-2013-3502 **Refs**: source, ref1
Hadoop YARN ResourceManager Unauthenticated Command Execution exploit/linux/http/hadoop_unauth_exec	2016-10-19	excellent	This module uses built-in functi execute arbitrary commands or Hadoop server which is not cor strong authentication, via Hado ResourceManager REST API. **Platforms**: linux **Refs**: source, ref1, ref2
HP System Management Anonymous Access Code Execution exploit/linux/http/hp_system_management	2012-09-01	normal	This module exploits an anonyr code execution on HP System 7.1.1 and earlier. The vulnerabi handling the iprange parameter against ... **Platforms**: linux **Refs**: source
Huawei HG532n Command Injection exploit/linux/http/huawei_hg532n_cmdinject	2017-04-15	excellent	This module exploits a commar vulnerability in the Huawei HG5 provided by TE-Data Egypt, lea shell. The router's web interfac of logins, a "limited" ... **Platforms**: linux **Refs**: source, ref1
IBM Data Risk Manager Unauthenticated Remote Code Execution exploit/linux/http/ibm_drm_rce	2020-04-21	excellent	IBM Data Risk Manager (IDRM vulnerabilities that can be chair unauthenticated attacker to ach code execution as root. The firs unauthenticated bypass, ... **Platforms**: linux **CVEs**: CVE-2020-4427, CVE-2 2020-4429, CVE-2020-4430 **Refs**: source, ref1, ref2, ref3
IBM QRadar SIEM Unauthenticated Remote Code Execution exploit/linux/http/ibm_qradar_unauth_rce	2018-05-28	excellent	IBM QRadar SIEM has three vu the Forensics web application t chained together allow an attac unauthenticated remote code e first stage bypasses ... **Platforms**: unix **CVEs**: CVE-2016-9722, CVE-2 2018-1612 **Refs**: source, ref1, ref2, ref3, re
Imperva SecureSphere PWS Command Injection exploit/linux/http/imperva_securesphere_exec	2018-10-08	excellent	This module exploits a commar vulnerability in Imperva Secure vulnerability exists in the PWS Python CGIs didn't properly sar supplied command ... **Platforms**: linux **Refs**: source

Metasploit Module	Date	Rank	Details
IPFire Bash Environment Variable Injection (Shellshock) exploit/linux/http/ipfire_bashbug_exec	2014-09-29	excellent	IPFire, a free linux based open distribution, version <= 2.15 Up contains an authenticated remc execution vulnerability via shell request headers. **Platforms**: linux, unix **CVEs**: CVE-2014-6271 **Refs**: source
IPFire proxy.cgi RCE exploit/linux/http/ipfire_oinkcode_exec	2017-06-09	excellent	IPFire, a free linux based open distribution, version < 2.19 Upd contains a remote command ex vulnerability in the ids.cgi page OINKCODE field. **Platforms**: unix **CVEs**: CVE-2017-9757 **Refs**: source
IPFire proxy.cgi RCE exploit/linux/http/ipfire_proxy_exec	2016-05-04	excellent	IPFire, a free linux based open distribution, version < 2.19 Upd contains a remote command ex vulnerability in the proxy.cgi pa **Platforms**: unix **Refs**: source
Jenkins CLI Deserialization exploit/linux/http/jenkins_cli_deserialization	2017-04-26	excellent	An unauthenticated Java objec vulnerability exists in the CLI cc Jenkins versions `v2.56` and b `readFrom` method within the ` in the Jenkins CLI ... **Platforms**: linux **CVEs**: CVE-2017-1000353 **Refs**: source, ref1, ref2
Kaltura Remote PHP Code Execution over Cookie exploit/linux/http/kaltura_unserialize_cookie_rce	2017-09-12	excellent	This module exploits an Object vulnerability in Kaltura. By expl vulnerability, unauthenticated u arbitrary code under the contex server user. Kaltura ... **Platforms**: php **CVEs**: CVE-2017-14143 **Refs**: source
Kaltura Remote PHP Code Execution exploit/linux/http/kaltura_unserialize_rce	2016-03-15	excellent	This module exploits an Object vulnerability in Kaltura. By expl vulnerability, unauthenticated u arbitrary code under the contex server user. Kaltura ... **Platforms**: php **Refs**: source
Klog Server authenticate.php user Unauthenticated Command Injection exploit/linux/http/klog_server_authenticate_user_unauth_command_injection	2020-12-27	excellent	This module exploits an unauth command injection vulnerability versions 2.4.1 and prior. The `a file uses the `user` HTTP POS call to the ... **Platforms**: linux, unix **CVEs**: CVE-2020-35729 **Refs**: source, ref1, ref2
Kloxo SQL Injection and Remote Code Execution exploit/linux/http/kloxo_sqli	2014-01-28	manual	This module exploits an unauth injection vulnerability affecting l exploited in the wild on January injection issue can be abused i retrieve the Kloxo ... **Platforms**: unix **Refs**: source, ref1, ref2, ref3
LibreNMS addhost Command Injection exploit/linux/http/librenms_addhost_cmd_inject	2018-12-16	excellent	This module exploits a commar vulnerability in the open source management software known a community parameter used in a to the addhost functionality is .. **Platforms**: unix **CVEs**: CVE-2018-20434 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
LibreNMS Collectd Command Injection exploit/linux/http/librenms_collectd_cmd_inject	2019-07-15	excellent	This module exploits a commar vulnerability in the Collectd gra functionality in LibreNMS. The parameters used to define the r are sanitized using the ... **Platforms**: unix **CVEs**: CVE-2019-10669 **Refs**: source, ref1
Linksys WRT54 Access Point apply.cgi Buffer Overflow exploit/linux/http/linksys_apply_cgi	2005-09-13	great	This module exploits a stack bu apply.cgi on the Linksys WRT5 WRT54GS routers. According t discovered this vulnerability, all versions prior to 4.20.7 and ... **Platforms**: linux **CVEs**: CVE-2005-2799 **Refs**: source, ref1
Linksys E1500/E2500 apply.cgi Remote Command Injection exploit/linux/http/linksys_e1500_apply_exec	2013-02-05	excellent	Some Linksys Routers are vuln authenticated OS command inj credentials for the web interfac admin/admin or admin/passwor blind os command injection ... **Platforms**: linux, unix **Refs**: source, ref1
Linksys E-Series TheMoon Remote Command Injection exploit/linux/http/linksys_themoon_exec	2014-02-13	excellent	Some Linksys E-Series Router to an unauthenticated OS comr This vulnerability was used fror "TheMoon" worm. There are m systems that are ... **Platforms**: linux, unix **Refs**: source, ref1, ref2
Linksys Devices pingstr Remote Command Injection exploit/linux/http/linksys_wrt110_cmd_exec	2013-07-12	excellent	The Linksys WRT100 and WRT routers are vulnerable to a com exploit in the ping field of the w **Platforms**: linux **CVEs**: CVE-2013-3568 **Refs**: source, ref1
Linksys WRT160nv2 apply.cgi Remote Command Injection exploit/linux/http/linksys_wrt160nv2_apply_exec	2013-02-11	excellent	Some Linksys Routers are vuln authenticated OS command inj web interface where default cre admin/admin or admin/passwor blind OS command ... **Platforms**: linux, unix **Refs**: source, ref1
Linksys WRT54GL apply.cgi Command Execution exploit/linux/http/linksys_wrt54gl_apply_exec	2013-01-18	manual	Some Linksys Routers are vuln authenticated OS command inj Interface. Default credentials ar or admin/password. Since it is a command injection ... **Platforms**: linux, unix **CVEs**: CVE-2005-2799 **Refs**: source, ref1
Linksys WVBR0-25 User-Agent Command Execution exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth	2017-12-13	excellent	The Linksys WVBR0-25 Wirele used by DirecTV to connect wir cable boxes to the Genie DVR, OS command injection in versi web management ... **Platforms**: unix **CVEs**: CVE-2017-17411 **Refs**: source, ref1
LinuxKI Toolset 6.01 Remote Command Execution exploit/linux/http/linuxki_rce	2020-05-17	excellent	This module exploits a vulnerab Toolset <= 6.01 which allows re execution. The kivis.php pid pa from the user is sent to the she resulting in ... **Platforms**: linux, php, unix **CVEs**: CVE-2020-7209 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Logsign Remote Command Injection exploit/linux/http/logsign_exec	2017-02-26	excellent	This module exploits a commar vulnerability in Logsign. By exp vulnerability, unauthenticated u arbitrary code under the root us a publicly ... **Platforms**: python **Refs**: source, ref1
Mailcleaner Remote Code Execution exploit/linux/http/mailcleaner_exec	2018-12-19	excellent	This module exploits the comm vulnerability of MailCleaner Co product. An authenticated user operating system command un the web server ... **Platforms**: python, unix **CVEs**: CVE-2018-20323 **Refs**: source, ref1
MicroFocus Secure Messaging Gateway Remote Code Execution exploit/linux/http/microfocus_secure_messaging_gateway	2018-06-19	excellent	This module exploits a SQL inj command injection vulnerability Secure Messaging Gateway. A unauthenticated user can exec command under the context of **Platforms**: php **CVEs**: CVE-2018-12464, CVE- **Refs**: source, ref1, ref2, ref3
Mida Solutions eFramework ajaxreq.php Command Injection exploit/linux/http/mida_solutions_eframework_ajaxreq_rce	2020-07-24	excellent	This module exploits a commar vulnerability in Mida Solutions e version 2.9.0 and prior. The `aj allows unauthenticated users to commands in the ... **Platforms**: linux, unix **CVEs**: CVE-2020-15920 **Refs**: source, ref1
MobileIron MDM Hessian-Based Java Deserialization RCE exploit/linux/http/mobileiron_mdm_hessian_rce	2020-09-12	excellent	This module exploits an ACL b MobileIron MDM products to ex gadget against a Hessian-base deserialization endpoint. **Platforms**: linux, unix **CVEs**: CVE-2020-15505 **Refs**: source, ref1, ref2, ref3
D-Link/TRENDnet NCC Service Command Injection exploit/linux/http/multi_ncc_ping_exec	2015-02-26	normal	This module exploits a remote injection vulnerability on severa vulnerability exists in the ncc se handling ping commands. This been tested on a DIR-626L ... **Platforms**: linux **CVEs**: CVE-2015-1187 **Refs**: source, ref1, ref2, ref3
MVPower DVR Shell Unauthenticated Command Execution exploit/linux/http/mvpower_dvr_shell_exec	2015-08-23	excellent	This module exploits an unauth command execution vulnerabili digital video recorders. The 'sh web interface executes arbitrar system commands ... **Platforms**: linux **Refs**: source, ref1, ref2
Nagios XI Authenticated Remote Command Execution exploit/linux/http/nagios_xi_authenticated_rce	2019-07-29	excellent	This module exploits a vulneral before 5.6.6 in order to execute commands as root. The module malicious plugin to the Nagios then executes this ... **Platforms**: linux, unix **CVEs**: CVE-2019-15949 **Refs**: source, ref1
Nagios XI Chained Remote Code Execution exploit/linux/http/nagios_xi_chained_rce	2016-03-06	excellent	This module exploits an SQL in bypass, file upload, command i privilege escalation in Nagios X a root shell. **Platforms**: unix **Refs**: source

Metasploit Module	Date	Rank	Details
Nagios XI Chained Remote Code Execution exploit/linux/http/nagios_xi_chained_rce_2_electric_boogaloo	2018-04-17	manual	This module exploits a few diffe vulnerabilities in Nagios XI 5.2. remote root access. The steps POST request to /nagiosql/adm which sets the ... **Platforms**: linux **CVEs**: CVE-2018-8733, CVE-2 2018-8735, CVE-2018-8736 **Refs**: source, ref1
Nagios XI Magpie_debug.php Root Remote Code Execution exploit/linux/http/nagios_xi_magpie_debug	2018-11-14	excellent	This module exploits two vulne Nagios XI <= 5.5.6: CVE-2018- allows for unauthenticated rem execution and CVE-2018-1571 for local privilege escalation. ... **Platforms**: linux **CVEs**: CVE-2018-15708, CVE- **Refs**: source, ref1, ref2
Netgear DGN1000B setup.cgi Remote Command Execution exploit/linux/http/netgear_dgn1000b_setup_exec	2013-02-06	excellent	Some Netgear Routers are vuln authenticated OS Command in vulnerability exists in the web in specifically in the setup.cgi com handling the TimeToLive ... **Platforms**: linux, unix **Refs**: source, ref1
Netgear DGN1000 Setup.cgi Unauthenticated RCE exploit/linux/http/netgear_dgn1000_setup_unauth_exec	2013-06-05	excellent	This module exploits an unauth command execution vulneralbil setup.cgi file in Netgear DGN1(versions up to 1.1.00.48, and D models. **Platforms**: linux **Refs**: source
Netgear DGN2200B pppoe.cgi Remote Command Execution exploit/linux/http/netgear_dgn2200b_pppoe_exec	2013-02-15	manual	Some Netgear Routers are vuln authenticated OS command inj web interface. Default credentia interface are admin/admin or a Since it is a blind ... **Platforms**: linux, unix **Refs**: source, ref1
Netgear DGN2200 dnslookup.cgi Command Injection exploit/linux/http/netgear_dnslookup_cmd_exec	2017-02-25	excellent	This module exploits a comma vulnerablity in NETGEAR DGN routers by sending a specially c request with valid login details. **Platforms**: unix **CVEs**: CVE-2017-6334 **Refs**: source
Netgear R7000 and R6400 cgi-bin Command Injection exploit/linux/http/netgear_r7000_cgibin_exec	2016-12-06	excellent	This module exploits an arbitra injection vulnerability in Netgea R6400 router firmware version and possibly earlier. **Platforms**: linux **CVEs**: CVE-2016-6277, CVE-2 **Refs**: source, ref1, ref2
NETGEAR ReadyNAS Perl Code Evaluation exploit/linux/http/netgear_readynas_exec	2013-07-12	manual	This module exploits a Perl coc NETGEAR ReadyNAS 4.2.23 a vulnerability exists on the web f specifically in the np_handler.p to an insecure usage ... **Platforms**: unix **CVEs**: CVE-2013-2751 **Refs**: source, ref1, ref2
Netgear Devices Unauthenticated Remote Command Execution exploit/linux/http/netgear_unauth_exec	2016-02-25	excellent	From the CVE-2016-1555 page boardData102.php, (2) boardD boardDataJP.php, (4) boardDat (5) boardDataWW.php in Netge before 3.3.3 and WN802Tv2, W **Platforms**: linux **CVEs**: CVE-2016-1555 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
NETGEAR WNR2000v5 (Un)authenticated hidden_lang_avi Stack Buffer Overflow exploit/linux/http/netgear_wnr2000_rce	2016-12-20	excellent	The NETGEAR WNR2000 rout buffer overflow vulnerability in t hidden_lang_avi parameter. In it is necessary to guess the val timestamp which is in ... **Platforms**: unix **CVEs**: CVE-2016-10174 **Refs**: source, ref1, ref2, ref3
Netsweeper WebAdmin unixlogin.php Python Code Injection exploit/linux/http/netsweeper_webadmin_unixlogin	2020-04-28	excellent	This module exploits a Python the Netsweeper WebAdmin cor unixlogin.php script, for version to execute code as the root use is bypassed by ... **Platforms**: python **CVEs**: CVE-2020-13167 **Refs**: source, ref1, ref2
Nginx HTTP Server 1.3.9-1.4.0 Chunked Encoding Stack Buffer Overflow exploit/linux/http/nginx_chunked_size	2013-05-07	great	This module exploits a stack bu versions 1.3.9 to 1.4.0 of nginx triggers an integer overflow in t ngx_http_parse_chunked() by s overly long hex value ... **Platforms**: unix **CVEs**: CVE-2013-2028 **Refs**: source, ref1
NUUO NVRmini 2 / Crystal / NETGEAR ReadyNAS Surveillance Authenticated Remote Code Execution exploit/linux/http/nuuo_nvrmini_auth_rce	2016-08-04	excellent	The NVRmini 2 Network Video Crystal NVR and the ReadyNA application are vulnerable to ar remote code execution on the e administration interface. An ... **Platforms**: unix **CVEs**: CVE-2016-5675 **Refs**: source, ref1, ref2
NUUO NVRmini 2 / NETGEAR ReadyNAS Surveillance Unauthenticated Remote Code Execution exploit/linux/http/nuuo_nvrmini_unauth_rce	2016-08-04	excellent	The NVRmini 2 Network Video the ReadyNAS Surveillance ap vulnerable to an unauthenticate execution on the exposed web interface. This results in ... **Platforms**: unix **CVEs**: CVE-2016-5674 **Refs**: source, ref1, ref2
op5 v7.1.9 Configuration Command Execution exploit/linux/http/op5_config_exec	2016-04-08	excellent	op5 an open source network m software. The configuration pag 7.1.9 and below allows the abil system command, which can b arbitrary code as an unpriv ... **Platforms**: linux, unix **Refs**: source, ref1
Openfiler v2.x NetworkCard Command Execution exploit/linux/http/openfiler_networkcard_exec	2012-09-04	excellent	This module exploits a vulnerat v2.x which could be abused to authenticated users to execute under the context of the 'openfi 'system.html' file ... **Platforms**: unix **Refs**: source, ref1
Pandora FMS Events Remote Command Execution exploit/linux/http/pandora_fms_events_exec	2020-06-04	excellent	This module exploits a vulnerat 13851) in Pandora FMS versio 7.0 NG 743, and 7.0 NG 744 (a versions) in order to execute ar commands. This module ... **Platforms**: linux, unix **CVEs**: CVE-2020-13851 **Refs**: source, ref1
Pandora FMS Remote Code Execution exploit/linux/http/pandora_fms_exec	2014-01-29	excellent	This module exploits a vulnerat Pandora FMS 5.0RC1 and low an unauthenticated command i Anyterm service on port 8023/T are executed as the ... **Platforms**: unix **Refs**: source

Metasploit Module	Date	Rank	Details
Pandora FMS Default Credential / SQLi Remote Code Execution exploit/linux/http/pandora_fms_sqli	2014-02-01	excellent	This module attempts to exploit in order to gain remote code ex Pandora FMS version <= 5.0 S attempt to authenticate using d is performed. ... **Platforms**: php **Refs**: source, ref1, ref2
Pandora FMS Ping Authenticated Remote Code Execution exploit/linux/http/pandora_ping_cmd_exec	2020-03-09	excellent	This module exploits a vulnerab Pandora FMS 7.0NG and lowe in Pandora FMS 7.0NG allows to execute arbitrary OS comma **Platforms**: linux **Refs**: source
Palo Alto Networks readSessionVarsFromFile() Session Corruption exploit/linux/http/panos_readsessionvars	2017-12-11	excellent	This module exploits a chain of Palo Alto Networks products ru versions prior to 6.1.19, 7.0.19, 8.0.6. This chain starts by using authentication bypass ... **Platforms**: unix **CVEs**: CVE-2017-15944 **Refs**: source, ref1
PeerCast URL Handling Buffer Overflow exploit/linux/http/peercast_url	2006-03-08	average	This module exploits a stack bu PeerCast <= v0.1216. The vuln caused due to a boundary erro handling of URL parameters. **Platforms**: linux **CVEs**: CVE-2006-1148 **Refs**: source
php imap_open Remote Code Execution exploit/linux/http/php_imap_open_rce	2018-10-23	good	The imap_open function within without the /norsh flag, will atte preauthenticate an IMAP sessi based systems, including Ubun mapped to the ssh binary. ... **Platforms**: unix **CVEs**: CVE-2018-19518, CVE- **Refs**: source, ref1, ref2, ref3
Hak5 WiFi Pineapple Preconfiguration Command Injection exploit/linux/http/pineapple_bypass_cmdinject	2015-08-01	excellent	This module exploits a login/cs vulnerability on WiFi Pineapple pineapple < 2.4. These devices identified by their SSID beacon 'Pineapple5_.', ... **Platforms**: unix **CVEs**: CVE-2015-4624 **Refs**: source
Hak5 WiFi Pineapple Preconfiguration Command Injection exploit/linux/http/pineapple_preconfig_cmdinject	2015-08-01	excellent	This module exploits a commar vulnerability on WiFi Pineapple pineapple < 2.4. We use a com default credentials with a weak csrf generation to ... **Platforms**: unix **CVEs**: CVE-2015-4624 **Refs**: source
PineApp Mail-SeCure livelog.html Arbitrary Command Execution exploit/linux/http/pineapp_livelog_exec	2013-07-26	excellent	This module exploits a commar vulnerability on PineApp Mail-S vulnerability exists on the livelo component, due to the insecure shell_exec() php function. ... **Platforms**: unix **Refs**: source
PineApp Mail-SeCure test_li_connection.php Arbitrary Command Execution exploit/linux/http/pineapp_test_li_conn_exec	2013-07-26	excellent	This module exploits a commar vulnerability on PineApp Mail-S vulnerability exists on the test_ component, due to the insecure system() php ... **Platforms**: unix **CVEs**: CVE-2013-6829 **Refs**: source

Metasploit Module	Date	Rank	Details
RedHat Piranha Virtual Server Package passwd.php3 Arbitrary Command Execution exploit/linux/http/piranha_passwd_exec	2000-04-04	excellent	This module abuses two flaws metacharacter injection vulnera HTTP management server of R systems running the Piranha L and GUI (rpm packages: piranh **Platforms**: unix **CVEs**: CVE-2000-0248, CVE-2 **Refs**: source
Pulse Secure VPN Arbitrary Command Execution exploit/linux/http/pulse_secure_cmd_exec	2019-04-24	excellent	This module exploits a post-aut injection in the Pulse Secure V execute commands as root. Th command is used to bypass ap whitelisting and run arbitrary ... **Platforms**: linux, unix **CVEs**: CVE-2019-11539 **Refs**: source, ref1, ref2, ref3
Pulse Secure VPN gzip RCE exploit/linux/http/pulse_secure_gzip_rce	2020-10-26	excellent	The Pulse Connect Secure app 9.1R9 suffers from an uncontro extraction vulnerability which al to overwrite arbitrary files, resu Code Execution as ... **Platforms**: linux, unix **CVEs**: CVE-2020-8260 **Refs**: source, ref1, ref2, ref3
QNAP Q'Center change_passwd Command Execution exploit/linux/http/qnap_qcenter_change_passwd_exec	2018-07-11	excellent	This module exploits a comma vulnerability in the `change_pas method within the web interface Q'Center virtual appliance vers 1.7.1083. The vulnerability ... **Platforms**: linux **CVEs**: CVE-2018-0706, CVE-2 **Refs**: source, ref1, ref2, ref3, re
Raidsonic NAS Devices Unauthenticated Remote Command Execution exploit/linux/http/raidsonic_nas_ib5220_exec_noauth	2013-02-04	manual	Different Raidsonic NAS device to OS command injection via th The vulnerability exists in timeh which is accessible without aut module has ... **Platforms**: unix **Refs**: source, ref1
Railo Remote File Include exploit/linux/http/railo_cfml_rfi	2014-08-26	excellent	This module exploits a remote vulnerability in Railo, tested aga 4.2.1. First, a call using a vulne thumbnail.cfm allows an attack an ... **Platforms**: unix **CVEs**: CVE-2014-5468 **Refs**: source, ref1
Rancher Server - Docker Exploit exploit/linux/http/rancher_server	2017-07-27	excellent	Utilizing Rancher Server, an att a docker container with the '/' p read/write permissions on the h running the docker container. A **Platforms**: linux **Refs**: source, ref1
Rconfig 3.x Chained Remote Code Execution exploit/linux/http/rconfig_ajaxarchivefiles_rce	2020-03-11	good	This module exploits multiple v rConfig version 3.9 in order to e commands. This module takes command injection vulnerability parameter ... **Platforms**: linux, unix **CVEs**: CVE-2019-19509, CVE- CVE-2020-10220 **Refs**: source, ref1, ref2
Realtek SDK Miniigd UPnP SOAP Command Execution exploit/linux/http/realtek_miniigd_upnp_exec_noauth	2015-04-24	normal	Different devices using the Rea the miniigd daemon are vulnera command injection in the UPnP Since it is a blind OS commanc vulnerability, there is no ... **Platforms**: linux **CVEs**: CVE-2014-8361 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Riverbed SteelCentral NetProfiler/NetExpress Remote Code Execution exploit/linux/http/riverbed_netprofiler_netexpress_exec	2016-06-27	excellent	This module exploits three sepa vulnerabilities found in the Rive SteelCentral NetProfiler/NetExp appliances to obtain remote co execution as the root user. A S **Platforms**: linux **Refs**: source, ref1
SaltStack Salt REST API Arbitrary Command Execution exploit/linux/http/saltstack_salt_api_cmd_exec	2020-11-03	excellent	This module exploits an authen and command injection in Salt REST API to execute comman user. The following versions ha patch: 2015.8.10, ... **Platforms**: linux, unix **CVEs**: CVE-2020-16846, CVE- **Refs**: source, ref1
SaltStack Salt API Unauthenticated RCE through wheel_async client exploit/linux/http/saltstack_salt_wheel_async_rce	2021-02-25	excellent	This module leverages an auth and directory traversal vulnerab Saltstack Salt's REST API to ex commands remotely on the `ma user. Every 60 seconds, ... **Platforms**: linux, unix **CVEs**: CVE-2021-25281, CVE- **Refs**: source, ref1, ref2
Seagate Business NAS Unauthenticated Remote Command Execution exploit/linux/http/seagate_nas_php_exec_noauth	2015-03-01	normal	Some Seagate Business NAS vulnerable to command execut include vulnerability hidden in t parameter of the CodeIgniter s The vulnerability ... **Platforms**: php **CVEs**: CVE-2014-8684, CVE-2 2014-8687 **Refs**: source, ref1, ref2
Supermicro Onboard IPMI close_window.cgi Buffer Overflow exploit/linux/http/smt_ipmi_close_window_bof	2013-11-06	good	This module exploits a buffer o Supermicro Onboard IPMI cont interface. The vulnerability exis close_window.cgi CGI applicati the insecure usage of ... **Platforms**: unix **CVEs**: CVE-2013-3623 **Refs**: source, ref1
Sophos Web Protection Appliance Interface Authenticated Arbitrary Command Execution exploit/linux/http/sophos_wpa_iface_exec	2014-04-08	excellent	This module takes advantage o vulnerabilities in order to gain r execution as root as an otherw privileged authorized user. By t of a mass assignment ... **Platforms**: unix **CVEs**: CVE-2014-2849, CVE-2 **Refs**: source, ref1
Sophos Web Protection Appliance sblistpack Arbitrary Command Execution exploit/linux/http/sophos_wpa_sblistpack_exec	2013-09-06	excellent	This module exploits a comma vulnerability on Sophos Web P Appliance 3.7.9, 3.8.0 and 3.8. vulnerability exists on the sblist reachable from the web ... **Platforms**: unix **CVEs**: CVE-2013-4983 **Refs**: source, ref1
Apache Spark Unauthenticated Command Execution exploit/linux/http/spark_unauth_rce	2017-12-12	excellent	This module exploits an unauth command execution vulnerabili Spark with standalone cluster r REST API. It uses the function CreateSubmissionRequest to s ... **Platforms**: java **CVEs**: CVE-2018-11770 **Refs**: source, ref1, ref2
Supervisor XML-RPC Authenticated Remote Code Execution exploit/linux/http/supervisor_xmlrpc_exec	2017-07-19	excellent	This module exploits a vulnerab Supervisor process control soft authenticated client can send a RPC request to supervisord tha arbitrary shell ... **Platforms**: linux **CVEs**: CVE-2017-11610 **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
Symantec Messaging Gateway Remote Code Execution exploit/linux/http/symantec_messaging_gateway_exec	2017-04-26	excellent	This module exploits the comm vulnerability of Symantec Mess product. An authenticated user terminal command under the c server user which is ... **Platforms**: python **CVEs**: CVE-2017-6326 **Refs**: source, ref1
Symantec Web Gateway 5.0.2.8 ipchange.php Command Injection exploit/linux/http/symantec_web_gateway_exec	2012-05-17	excellent	This module exploits a comma vulnerability found in Symantec HTTP service due to the insecu exec() function. This module ab spywall/ipchange.php file ... **Platforms**: unix **CVEs**: CVE-2012-0297 **Refs**: source, ref1
Symantec Web Gateway 5.0.2.8 Arbitrary PHP File Upload Vulnerability exploit/linux/http/symantec_web_gateway_file_upload	2012-05-17	excellent	This module exploits a file uplo found in Symantec Web Gatew service. Due to the incorrect us extensions in the upload_file() attackers may to abuse the ... **Platforms**: php **CVEs**: CVE-2012-0299 **Refs**: source, ref1
Symantec Web Gateway 5.0.2.8 relfile File Inclusion Vulnerability exploit/linux/http/symantec_web_gateway_lfi	2012-05-17	excellent	This module exploits a vulnerab Symantec Web Gateway's HTT injecting PHP code in the acce possible to load it with a directo which allows ... **Platforms**: php **CVEs**: CVE-2012-0297 **Refs**: source, ref1
Symantec Web Gateway 5.0.2.18 pbcontrol.php Command Injection exploit/linux/http/symantec_web_gateway_pbcontrol	2012-07-23	excellent	This module exploits a comma vulnerability found in Symantec HTTP service. While handling t parameter, the Spywall API doe filtering before passing it ... **Platforms**: unix **CVEs**: CVE-2012-2953 **Refs**: source, ref1
Symantec Web Gateway 5 restore.php Post Authentication Command Injection exploit/linux/http/symantec_web_gateway_restore	2014-12-16	excellent	This module exploits a comma vulnerability found in Symantec setting restoration feature. The can be used to inject system co syscall function, ... **Platforms**: unix **CVEs**: CVE-2014-7285 **Refs**: source, ref1, ref2
Synology DiskStation Manager SLICEUPLOAD Remote Command Execution exploit/linux/http/synology_dsm_sliceupload_exec_noauth	2013-10-31	excellent	This module exploits a vulnerab Synology DiskStation Manager 4.x, which allows the execution commands under root privilege vulnerability is located in ... **Platforms**: unix **CVEs**: CVE-2013-6955 **Refs**: source
Synology DiskStation Manager smart.cgi Remote Command Execution exploit/linux/http/synology_dsm_smart_exec_auth	2017-11-08	excellent	This module exploits a vulnerab Synology DiskStation Manager < 5.2-5967-5, which allows the arbitrary commands under root website ... **Platforms**: python **CVEs**: CVE-2017-15889 **Refs**: source, ref1, ref2
TP-Link Cloud Cameras NCXXX Bonjour Command Injection exploit/linux/http/tp_link_ncxxx_bonjour_command_injection	2020-04-29	excellent	TP-Link cloud cameras NCXXX NC210, NC220, NC230, NC25(NC450) are vulnerable to an au command injection. In all devic NC210, despite a check on the **Platforms**: linux **CVEs**: CVE-2020-12109, CVE- **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
TP-Link SC2020n Authenticated Telnet Injection exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection	2015-12-20	excellent	The TP-Link SC2020n Network is vulnerable to OS Command web interface. By firing up the t is possible to gain root on the d vulnerability ... **Platforms**: unix **CVEs**: CVE-2013-2578 **Refs**: source
Zyxel/Eir D1000 DSL Modem NewNTPServer Command Injection Over TR-064 exploit/linux/http/tr064_ntpserver_cmdinject	2016-11-07	normal	Broadband DSL modems manu Zyxel and distributed by some I are vulnerable to a command in vulnerability when setting the 'N value using the TR-64 SOAP-b **Platforms**: linux **CVEs**: CVE-2016-10372 **Refs**: source, ref1, ref2, ref3
Trend Micro InterScan Messaging Security (Virtual Appliance) Remote Code Execution exploit/linux/http/trendmicro_imsva_widget_exec	2017-10-07	excellent	This module exploits the authe and command injection vulnera Unauthenticated users can exe command under the context of user. The ... **Platforms**: python **Refs**: source, ref1, ref2
Trend Micro Smart Protection Server Exec Remote Code Injection exploit/linux/http/trendmicro_sps_exec	2016-08-08	excellent	This module exploits a vulneral TrendMicro Smart Protection S untrusted inputs are fed to Serv system command, leading to co injection. Please note: ... **Platforms**: linux **CVEs**: CVE-2016-6267 **Refs**: source
Trend Micro Web Security (Virtual Appliance) Remote Code Execution exploit/linux/http/trendmicro_websecurity_exec	2020-06-10	excellent	This module exploits multiple v together in order to achive a re execution. Unauthenticated use terminal command under the co user. The ... **Platforms**: python **CVEs**: CVE-2020-8604, CVE-2020-8606 **Refs**: source
Trend Micro InterScan Messaging Security (Virtual Appliance) Remote Code Execution exploit/linux/http/trend_micro_imsva_exec	2017-01-15	excellent	This module exploits a comma vulnerability in the Trend Micro An authenticated user can exec command under the context of user which is root. ... **Platforms**: python **CVEs**: CVE-2017-6398 **Refs**: source, ref1
TrueOnline / Billion 5200W-T Router Unauthenticated Command Injection exploit/linux/http/trueonline_billion_5200w_rce	2016-12-26	excellent	TrueOnline is a major ISP in Th distributes a customized versio 5200W-T router. This customiz least two command injection vu ... **Platforms**: unix **CVEs**: CVE-2017-18369, CVE- **Refs**: source, ref1, ref2, ref3
TrueOnline / ZyXEL P660HN-T v1 Router Unauthenticated Command Injection exploit/linux/http/trueonline_p660hn_v1_rce	2016-12-26	excellent	TrueOnline is a major ISP in Th distributes a customized versio P660HN-T v1 router. This custo has an unauthenticated comma vulnerability in the ... **Platforms**: unix **CVEs**: CVE-2017-18368 **Refs**: source, ref1, ref2, ref3
TrueOnline / ZyXEL P660HN-T v2 Router Authenticated Command Injection exploit/linux/http/trueonline_p660hn_v2_rce	2016-12-26	excellent	TrueOnline is a major ISP in Th distributes a customized versio P660HN-T v2 router. This custo has an authenticated command vulnerability in the ... **Platforms**: linux **CVEs**: CVE-2017-18370, CVE- **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Ubiquiti airOS Arbitrary File Upload exploit/linux/http/ubiquiti_airos_file_upload	2016-02-13	excellent	This module exploits a pre-auth install a new root user to /etc/p SSH key to /etc/dropbear/autho /etc/{passwd,dropbear/authoriz overwritten. ... **Platforms**: unix **Refs**: source
Unitrends UEB http api remote code execution exploit/linux/http/ueb_api_rce	2017-08-08	excellent	It was discovered that the api/s interface in Unitrends Backup (10.0.0 has an issue in which or parameters was not validated. attacker could use this flaw ... **Platforms**: linux **CVEs**: CVE-2017-12478, CVE- **Refs**: source, ref1, ref2, ref3, re
Unraid 6.8.0 Auth Bypass PHP Code Execution exploit/linux/http/unraid_auth_bypass_exec	2020-02-10	excellent	This module exploits two vulne Unraid 6.8.0. An authentication to gain access to the administra and an insecure use of the extr can ... **Platforms**: php **CVEs**: CVE-2020-5847, CVE-2 **Refs**: source, ref1, ref2
Arris VAP2500 tools_command.php Command Execution exploit/linux/http/vap2500_tools_command_exec	2014-11-25	normal	Arris VAP2500 access points a OS command injection in the w portal via the tools_command.p Though authentication is requir page, it is trivially ... **Platforms**: unix **CVEs**: CVE-2014-8423, CVE-2 **Refs**: source, ref1
Vesta Control Panel Authenticated Remote Code Execution exploit/linux/http/vestacp_exec	2020-03-17	excellent	This module exploits an authen command injection vulnerability user-backups bash script file in Panel to gain remote code exe user. **Platforms**: python **CVEs**: CVE-2020-10808 **Refs**: source, ref1
VMware View Planner Unauthenticated Log File Upload RCE exploit/linux/http/vmware_view_planner_4_6_uploadlog_rce	2021-03-02	excellent	This module exploits an unauth upload within the log_upload_w VMWare View Planner 4.6 prio Patch 1. Successful exploitatio RCE as the ... **Platforms**: python **CVEs**: CVE-2021-21978 **Refs**: source, ref1, ref2
WAN Emulator v2.3 Command Execution exploit/linux/http/wanem_exec	2012-08-12	excellent	This module exploits a comma vulnerability in WAN Emulator v can be abused to allow unauth to execute arbitrary commands context of the 'www-data' ... **Platforms**: unix **Refs**: source
Western Digital MyCloud multi_uploadify File Upload Vulnerability exploit/linux/http/wd_mycloud_multiupload_upload	2017-07-29	excellent	This module exploits a file uplo found in Western Digital's MyC administration HTTP service. T /web/jquery/uploader/multi_upl script provides multipart ... **Platforms**: php **CVEs**: CVE-2017-17560 **Refs**: source, ref1, ref2, ref3
WebCalendar 1.2.4 Pre-Auth Remote Code Injection exploit/linux/http/webcalendar_settings_exec	2012-04-23	excellent	This module exploits a vulnerab k5n.us WebCalendar, version 1 not removed, the settings.php s installation can be update by a then inject ... **Platforms**: linux, unix **CVEs**: CVE-2012-1495 **Refs**: source

Metasploit Module	Date	Rank	Details
WeBid converter.php Remote PHP Code Injection exploit/linux/http/webid_converter	2011-07-05	excellent	This module exploits a vulnerat WeBid version 1.0.2. By abusir converter.php file, a malicious u PHP code in the includes/curre without any ... **Platforms**: php **Refs**: source, ref1
Webmin password_change.cgi Backdoor exploit/linux/http/webmin_backdoor	2019-08-10	excellent	This module exploits a backdoc versions 1.890 through 1.920. (SourceForge downloads were l they are listed as official downl project's site. Unknown ... **Platforms**: linux, unix **CVEs**: CVE-2019-15107 **Refs**: source, ref1, ref2, ref3, re
Webmin Package Updates Remote Command Execution exploit/linux/http/webmin_packageup_rce	2019-05-16	excellent	This module exploits an arbitra execution vulnerability in Webn lower versions. Any user autho "Package Updates" module car arbitrary commands with root .. **Platforms**: unix **CVEs**: CVE-2019-12840 **Refs**: source, ref1
Barco WePresent file_transfer.cgi Command Injection exploit/linux/http/wepresent_cmd_injection	-	excellent	This module exploits an unauth command injection vulnerability WePresent and related OEM'ec vulnerability is triggered via an request to the ... **Platforms**: linux, unix **CVEs**: CVE-2019-3929 **Refs**: source, ref1
WePresent WiPG-1000 Command Injection exploit/linux/http/wipg1000_cmd_injection	2017-04-20	excellent	This module exploits a commar vulnerability in an undocumente several versions of the WePres devices. Version 2.0.0.7 was cc vulnerable, 2.2.3.0 patched ... **Platforms**: unix **Refs**: source, ref1
Xplico Remote Code Execution exploit/linux/http/xplico_exec	2017-10-29	excellent	This module exploits command vulnerability. Unauthenticated u a new account and then execut command under the context of The specific flaw exists ... **Platforms**: unix **CVEs**: CVE-2017-16666 **Refs**: source, ref1, ref2
Zabbix 2.0.8 SQL Injection and Remote Code Execution exploit/linux/http/zabbix_sqli	2013-09-23	excellent	This module exploits an unauth injection vulnerability affecting 2.0.8 and lower. The SQL injec abused in order to retrieve an a If an ... **Platforms**: unix **CVEs**: CVE-2013-5743 **Refs**: source, ref1
Zenoss 3 showDaemonXMLConfig Command Execution exploit/linux/http/zenoss_showdaemonxmlconfig_exec	2012-07-30	good	This module exploits a commar vulnerability in Zenoss 3.x whic abused to allow authenticated u arbitrary code under the contex user. The ... **Platforms**: unix **Refs**: source, ref1
ZEN Load Balancer Filelog Command Execution exploit/linux/http/zen_load_balancer_exec	2012-09-14	excellent	This module exploits a vulnerat Balancer version 2.0 and 3.0-rc abused to allow authenticated u arbitrary code under the contex user. ... **Platforms**: unix **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Zimbra Collaboration Autodiscover Servlet XXE and ProxyServlet SSRF exploit/linux/http/zimbra_xxe_rce	2019-03-13	excellent	This module exploits an XML e vulnerability and a server side r get unauthenticated code exec Collaboration Suite. The XML e vulnerability ... **Platforms**: linux **CVEs**: CVE-2019-9621, CVE-2 **Refs**: source, ref1
AlienVault OSSIM av-centerd Command Injection exploit/linux/ids/alienvault_centerd_soap_exec	2014-05-05	excellent	This module exploits a code ex AlienVault 4.6.1 and prior. The exists in the av-centerd SOAP where the update_system_info_debian_p uses perl ... **Platforms**: unix **CVEs**: CVE-2014-3804 **Refs**: source, ref1
Snort Back Orifice Pre-Preprocessor Buffer Overflow exploit/linux/ids/snortbopre	2005-10-18	good	This module exploits a stack bu the Back Orifice pre-processor with Snort versions 2.4.0, 2.4.1 2.4.3. This vulnerability could b completely ... **Platforms**: linux **CVEs**: CVE-2005-3252 **Refs**: source
UoW IMAP Server LSUB Buffer Overflow exploit/linux/imap/imap_uw_lsub	2000-04-16	good	This module exploits a buffer o 'LSUB' command of the Univers Washington IMAP service. This only be exploited with a valid us password. **Platforms**: linux **CVEs**: CVE-2000-0284 **Refs**: source
Desktop Linux Password Stealer and Privilege Escalation exploit/linux/local/desktop_privilege_escalation	2014-08-07	excellent	This module steals the user pa administrative user on a deskto when it is entered for unlocking doing administrative actions us Then, it ... **Platforms**: linux **Refs**: source
Linux Nested User Namespace idmap Limit Local Privilege Escalation exploit/linux/local/nested_namespace_idmap_limit_priv_esc	2018-11-15	great	This module exploits a vulnerab kernels 4.15.0 to 4.18.18, and 4 where broken uid/gid mappings user namespaces and kernel u allow elevation ... **Platforms**: linux **CVEs**: CVE-2018-18955 **Refs**: source, ref1, ref2, ref3, re ref7, ref8, ref9
ABRT raceabrt Privilege Escalation exploit/linux/local/abrt_raceabrt_priv_esc	2015-04-14	excellent	This module attempts to gain ro Linux systems with a vulnerable Automatic Bug Reporting Tool (configured as the crash handle condition allows local users to . **Platforms**: linux **CVEs**: CVE-2015-1862, CVE-2 **Refs**: source, ref1, ref2, ref3, re ref7, ref8, ref9, ref10
ABRT sosreport Privilege Escalation exploit/linux/local/abrt_sosreport_priv_esc	2015-11-23	excellent	This module attempts to gain ro RHEL systems with a vulnerab Automatic Bug Reporting Tool (configured as the crash handle uses an insecure temporary ... **Platforms**: linux **CVEs**: CVE-2015-5287 **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
AF_PACKET chocobo_root Privilege Escalation exploit/linux/local/af_packet_chocobo_root_priv_esc	2016-08-12	good	This module exploits a race cor after-free in the packet_set_ring net/packet/af_packet.c (AF_PA Linux kernel to execute code as 2016-8655). The bug was ... **Platforms**: linux **CVEs**: CVE-2016-8655 **Refs**: source, ref1, ref2, ref3, re ref7
AF_PACKET packet_set_ring Privilege Escalation exploit/linux/local/af_packet_packet_set_ring_priv_esc	2017-03-29	good	This module exploits a heap-ou in the packet_set_ring function net/packet/af_packet.c (AF_PA Linux kernel to execute code as 2017-7308). The bug was ... **Platforms**: linux **CVEs**: CVE-2017-7308 **Refs**: source, ref1, ref2, ref3, re
Apport / ABRT chroot Privilege Escalation exploit/linux/local/apport_abrt_chroot_priv_esc	2015-03-31	excellent	This module attempts to gain ro Linux systems by invoking the handler inside a namespace ("c Apport versions 2.13 through 2 2.17.1 on Ubuntu ... **Platforms**: linux **CVEs**: CVE-2015-1318 **Refs**: source, ref1, ref2, ref3, re ref7, ref8
APT Package Manager Persistence exploit/linux/local/apt_package_manager_persistence	1999-03-09	excellent	This module will run a payload package manager is used. No l automatically so you must conf appropriate exploit/multi/handle This module creates a ... **Platforms**: linux, unix **Refs**: source, ref1
AddressSanitizer (ASan) SUID Executable Privilege Escalation exploit/linux/local/asan_suid_executable_priv_esc	2016-02-17	excellent	This module attempts to gain ro Linux systems using setuid exe compiled with AddressSanitizer configuration related environme permitted when ... **Platforms**: linux **Refs**: source, ref1, ref2, ref3, re
Autostart Desktop Item Persistence exploit/linux/local/autostart_persistence	2006-02-13	excellent	This module will create an auto execute a payload. The payloa executed when the users logs i **Platforms**: linux, unix **Refs**: source
Bash Profile Persistence exploit/linux/local/bash_profile_persistence	1989-06-08	normal	This module writes an executio target's Bash profile. The execu executes a call back payload w target user opens a Bash termi not run ... **Platforms**: linux, unix **Refs**: source, ref1
blueman set_dhcp_handler D-Bus Privilege Escalation exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc	2015-12-18	excellent	This module attempts to gain ro exploiting a Python code injecti in blueman versions prior to 2.0 `org.blueman.Mechanism.Enab Bus interface exposes ... **Platforms**: linux **CVEs**: CVE-2015-8612 **Refs**: source, ref1, ref2, ref3, re
Linux BPF doubleput UAF Privilege Escalation exploit/linux/local/bpf_priv_esc	2016-05-04	good	Linux kernel 4.4 < 4.5.5 extend Packet Filter (eBPF) does not p reference count file descriptors use-after-free, which can be ab privileges. The ... **Platforms**: linux **CVEs**: CVE-2016-4557 **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
Linux BPF Sign Extension Local Privilege Escalation exploit/linux/local/bpf_sign_extension_priv_esc	2017-11-12	great	Linux kernel prior to 4.14.8 con vulnerability in the Berkeley Pa verifier. The `check_alu_op` fur incorrect sign extension which to be ... **Platforms**: linux **CVEs**: CVE-2017-16995 **Refs**: source, ref1, ref2, ref3, re ref7, ref8, ref9, ref10, ref11
Cisco Prime Infrastructure Runrshell Privilege Escalation exploit/linux/local/cpi_runrshell_priv_esc	2018-12-08	excellent	This modules exploits a vulnera Prime Infrastructure's runrshell runrshell binary is meant to exe script as root, but can be abuse commands in ... **Platforms**: linux **Refs**: source, ref1
Cron Persistence exploit/linux/local/cron_persistence	1979-07-01	excellent	This module will create a cron c to execute a payload. The mod ability to automatically clean up prevent multiple executions. sy copy of ... **Platforms**: linux, unix **Refs**: source
Diamorphine Rootkit Signal Privilege Escalation exploit/linux/local/diamorphine_rootkit_signal_priv_esc	2013-11-07	excellent	This module uses Diamorphine feature using signal 64 to eleva of arbitrary processes to UID 0 module has been tested succes Diamorphine from ... **Platforms**: linux **Refs**: source, ref1
Docker Daemon Privilege Escalation exploit/linux/local/docker_daemon_privilege_escalation	2016-06-28	excellent	This module obtains root privile host account with access to the daemon. Usually this includes a `docker` group. **Platforms**: linux **Refs**: source
Docker Privileged Container Escape exploit/linux/local/docker_privileged_container_escape	2019-07-17	normal	This module escapes from a pr container and obtains root on th by abusing the Linux cgroup nc release feature. This exploit sh any container ... **Platforms**: linux **Refs**: source, ref1, ref2
Exim 4.87 - 4.91 Local Privilege Escalation exploit/linux/local/exim4_deliver_message_priv_esc	2019-06-05	excellent	This module exploits a flaw in E 4.87 to 4.91 (inclusive). Improp recipient address in deliver_me in /src/deliver.c may lead to cor with root ... **Platforms**: linux **CVEs**: CVE-2019-10149 **Refs**: source, ref1
glibc LD_AUDIT Arbitrary DSO Load Privilege Escalation exploit/linux/local/glibc_ld_audit_dso_load_priv_esc	2010-10-18	excellent	This module attempts to gain ro Linux systems by abusing a vu GNU C Library (glibc) dynamic in versions before 2.11.3, and 2 2.12.2 ... **Platforms**: linux **CVEs**: CVE-2010-3847, CVE-2 **Refs**: source, ref1, ref2, ref3, re ref7
glibc '$ORIGIN' Expansion Privilege Escalation exploit/linux/local/glibc_origin_expansion_priv_esc	2010-10-18	excellent	This module attempts to gain ro Linux systems by abusing a vu GNU C Library (glibc) dynamic `ld.so` versions before 2.11.3, a 2.12.2 ... **Platforms**: linux **CVEs**: CVE-2010-3847 **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
glibc 'realpath()' Privilege Escalation exploit/linux/local/glibc_realpath_priv_esc	2018-01-16	normal	This module attempts to gain r Linux systems by abusing a vu C Library (glibc) version 2.26 a module uses halfdog's Rationa exploit a ... **Platforms**: linux **CVEs**: CVE-2018-1000001 **Refs**: source, ref1, ref2, ref3, r
HP System Management Homepage Local Privilege Escalation exploit/linux/local/hp_smhstart	2013-03-30	normal	Versions of HP System Manag Homepage <= 7.1.2 include a s smhstart which is vulnerable to overflow in SSL_SHARE_BASI variable. **Platforms**: linux **Refs**: source
HP Performance Monitoring xglance Priv Esc exploit/linux/local/hp_xglance_priv_esc	2014-11-19	great	This exploit takes advantage of part of HP's Glance (or Perform version 11 'and subsequent' , w compiled with an insecure RPA RPATH includes a ... **Platforms**: linux **CVEs**: CVE-2014-2630 **Refs**: source, ref1, ref2, ref3, r
Juju-run Agent Privilege Escalation exploit/linux/local/juju_run_agent_priv_esc	2017-04-13	excellent	This module attempts to gain r Juju agent systems running the utility. Juju agent systems runn prior to version 1.25.12, 2.0.x b 2.1.x ... **Platforms**: linux **CVEs**: CVE-2017-9232 **Refs**: source, ref1
Kloxo Local Privilege Escalation exploit/linux/local/kloxo_lxsuexec	2012-09-18	excellent	Version 6.1.12 and earlier of Kl setuid root binaries such as lxs lxrestart, allow local privilege e from uid 48, Apache by default the ... **Platforms**: linux **Refs**: source, ref1
ktsuss suid Privilege Escalation exploit/linux/local/ktsuss_suid_priv_esc	2011-08-13	excellent	This module attempts to gain r exploiting a vulnerability in ktsu and prior. The ktsuss executab and does not drop privileges pr user ... **Platforms**: linux **CVEs**: CVE-2011-2921 **Refs**: source, ref1, ref2, ref3
lastore-daemon D-Bus Privilege Escalation exploit/linux/local/lastore_daemon_dbus_priv_esc	2016-02-02	excellent	This module attempts to gain r Deepin Linux systems by using to install a package. The lastor configuration on Deepin Linux p in the sudo ... **Platforms**: linux **Refs**: source, ref1
Libuser roothelper Privilege Escalation exploit/linux/local/libuser_roothelper_priv_esc	2015-07-24	great	This module attempts to gain r Red Hat based Linux systems, Fedora and CentOS, by exploit injection vulnerability in libuser versions ... **Platforms**: linux **CVEs**: CVE-2015-3245, CVE-2 **Refs**: source, ref1, ref2
Linux Kernel 4.6.3 Netfilter Privilege Escalation exploit/linux/local/netfilter_priv_esc_ipv4	2016-06-03	good	This module attempts to exploit on Linux Kernels before 4.6.3, only works against Ubuntu 16.0 with kernel 4.4.0-21-generic. S have to be ... **Platforms**: linux **CVEs**: CVE-2016-4997, CVE-2 2016-49972016 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Network Manager VPNC Username Privilege Escalation exploit/linux/local/network_manager_vpnc_username_priv_esc	2018-07-26	excellent	This module exploits an injectio the Network Manager VPNC pl privileges. This module uses a vulnerability in the configured u VPN ... **Platforms**: linux **CVEs**: CVE-2018-10900 **Refs**: source, ref1, ref2, ref3, re ref7, ref8, ref9
Debian/Ubuntu ntfs-3g Local Privilege Escalation exploit/linux/local/ntfs3g_priv_esc	2017-01-05	good	ntfs-3g mount helper in Ubuntu Debian 7, 8, and possibly 9 doe sanitize the environment when modprobe. This can be abused module and execute a ... **Platforms**: linux **CVEs**: CVE-2017-0358 **Refs**: source, ref1
Micro Focus (HPE) Data Protector SUID Privilege Escalation exploit/linux/local/omniresolve_suid_priv_esc	2019-09-13	excellent	This module exploits the truste environment variable of the SU `omniresolve` in Micro Focus (H Protector A.10.40 and prior. Th executable calls the ... **Platforms**: linux **CVEs**: CVE-2019-11660 **Refs**: source, ref1
Overlayfs Privilege Escalation exploit/linux/local/overlayfs_priv_esc	2015-06-16	good	This module attempts to exploit CVEs related to overlayfs. CVE Ubuntu specific -> 3.13.0-24 (1 3.13.0-55 3.16.0-25 (14.10 defa 3.19.0-18 (15.04 ... **Platforms**: linux **CVEs**: CVE-2015-1328, CVE-2 2015-13281328, CVE-2015-86 **Refs**: source
Linux PolicyKit Race Condition Privilege Escalation exploit/linux/local/pkexec	2011-04-01	great	A race condition flaw was found pkexec utility and polkitd daem could use this flaw to appear as user to pkexec, allowing them t arbitrary ... **Platforms**: linux **CVEs**: CVE-2011-1485 **Refs**: source
ptrace Sudo Token Privilege Escalation exploit/linux/local/ptrace_sudo_token_priv_esc	2019-03-24	excellent	This module attempts to gain ro blindly injecting into the session shell processes and executing calling `system()`, in the hope t has valid ... **Platforms**: linux **Refs**: source, ref1, ref2, ref3, re ref7
Linux Polkit pkexec helper PTRACE_TRACEME local root exploit exploit/linux/local/ptrace_traceme_pkexec_helper	2019-07-04	excellent	This module exploits an issue i kernel/ptrace.c before Linux ke issue can be exploited from a L terminal, but not over an SSH s requires ... **Platforms**: linux **CVEs**: CVE-2019-13272 **Refs**: source, ref1, ref2
rc.local Persistence exploit/linux/local/rc_local_persistence	1980-10-01	excellent	This module will edit /etc/rc.loca persist a payload. The payload on the next reboot. **Platforms**: linux, unix **Refs**: source
Reliable Datagram Sockets (RDS) rds_atomic_free_op NULL pointer dereference Privilege Escalation exploit/linux/local/rds_atomic_free_op_null_pointer_deref_priv_esc	2018-11-01	good	This module attempts to gain ro Linux systems by abusing a NU dereference in the `rds_atomic_ function in the Reliable Datagra (RDS) kernel module (rds.ko). **Platforms**: linux **CVEs**: CVE-2018-5333, CVE-2 **Refs**: source, ref1, ref2, ref3, re ref7

Metasploit Module	Date	Rank	Details
Reliable Datagram Sockets (RDS) rds_page_copy_user Privilege Escalation exploit/linux/local/rds_rds_page_copy_user_priv_esc	2010-10-20	great	This module exploits a vulnerat `rds_page_copy_user` function `net/rds/page.c` (RDS) in Linux 2.6.30 to 2.6.36-rc8 to execute (CVE-2010-3904). This module **Platforms**: linux **CVEs**: CVE-2010-3904 **Refs**: source, ref1, ref2, ref3, re
Linux Kernel recvmmsg Privilege Escalation exploit/linux/local/recvmmsg_priv_esc	2014-02-02	good	This module attempts to exploit 0038, by sending a recvmmsg a crafted timeout pointer param This exploit has offsets for 3 Ub ... **Platforms**: linux **CVEs**: CVE-2014-0038 **Refs**: source, ref1
Reptile Rootkit reptile_cmd Privilege Escalation exploit/linux/local/reptile_rootkit_reptile_cmd_priv_esc	2018-10-29	excellent	This module uses Reptile rootk backdoor executable to gain ro using the `root` command. This been tested successfully with R `master` branch ... **Platforms**: linux **Refs**: source, ref1, ref2
Service Persistence exploit/linux/local/service_persistence	1983-01-01	excellent	This module will create a servic and mark it for auto-restart. We access to write service files and restart services Targets: Syster 5 Debian <= 6 ... **Platforms**: linux, unix **Refs**: source, ref1
Serv-U FTP Server prepareinstallation Privilege Escalation exploit/linux/local/servu_ftp_server_prepareinstallation_priv_esc	2019-06-05	excellent	This module attempts to gain ro systems running Serv-U FTP S prior to 15.1.7. The `Serv-U` ex setuid `root`, and uses `ARGV[ `system()`, ... **Platforms**: linux **CVEs**: CVE-2019-12181 **Refs**: source, ref1, ref2, ref3, re
Linux Kernel Sendpage Local Privilege Escalation exploit/linux/local/sock_sendpage	2009-08-13	great	The Linux kernel failed to prope some entries in the proto_ops s protocols, leading to NULL beir and used as a function pointer. mmap(2) to map ... **Platforms**: linux **CVEs**: CVE-2009-2692 **Refs**: source, ref1, ref2
Sophos Web Protection Appliance clear_keys.pl Local Privilege Escalation exploit/linux/local/sophos_wpa_clear_keys	2013-09-06	excellent	This module abuses a commar the clear_keys.pl perl script, ins Sophos Web Protection Applia privileges from the "spiderman" This module is ... **Platforms**: linux **CVEs**: CVE-2013-4984 **Refs**: source, ref1
Sudo Heap-Based Buffer Overflow exploit/linux/local/sudo_baron_samedit	2021-01-26	excellent	A heap based buffer overflow e command line utility that can be local attacker to gain elevated p vulnerability was introduced in ... **Platforms**: linux, unix **CVEs**: CVE-2021-3156 **Refs**: source, ref1, ref2, ref3, re
Login to Another User with Su on Linux / Unix Systems exploit/linux/local/su_login	1971-11-03	normal	This module attempts to create session by invoking the su com username and password. If the successful, a new session is cr specified payload. Because ... **Platforms**: linux, unix **Refs**: source

Metasploit Module	Date	Rank	Details
SystemTap MODPROBE_OPTIONS Privilege Escalation exploit/linux/local/systemtap_modprobe_options_priv_esc	2010-11-17	excellent	This module attempts to gain rc exploiting a vulnerability in the executable included with Syste 1.3. The `staprun` executable c environment ... **Platforms**: linux **CVEs**: CVE-2010-4170 **Refs**: source, ref1, ref2, ref3, re
Linux udev Netlink Local Privilege Escalation exploit/linux/local/udev_netlink	2009-04-16	great	Versions of udev < 1.4.1 do not netlink messages are coming fr This allows local users to gain p sending netlink messages from **Platforms**: linux **CVEs**: CVE-2009-1185 **Refs**: source
Unitrends Enterprise Backup bpserverd Privilege Escalation exploit/linux/local/ueb_bpserverd_privesc	2018-03-14	excellent	It was discovered that the Unitr proprietary protocol, as expose an issue in which its authentica bypassed. A remote attacker co issue to execute ... **Platforms**: linux **CVEs**: CVE-2018-6329 **Refs**: source, ref1, ref2
Linux Kernel UDP Fragmentation Offset (UFO) Privilege Escalation exploit/linux/local/ufo_privilege_escalation	2017-08-10	good	This module attempts to gain rc Linux systems by abusing UDP Offload (UFO). This exploit targ using Ubuntu (Trusty / Xenial) k <= 4.4.0-89 ... **Platforms**: linux **CVEs**: CVE-2017-1000112 **Refs**: source, ref1, ref2, ref3, re ref7
VMware Workstation ALSA Config File Local Privilege Escalation exploit/linux/local/vmware_alsa_config	2017-05-22	excellent	This module exploits a vulnerab Workstation Pro and Player on allows users to escalate their p an ALSA configuration file to lo shared ... **Platforms**: linux **CVEs**: CVE-2017-4915 **Refs**: source, ref1, ref2, ref3, re
VMWare Setuid vmware-mount Unsafe popen(3) exploit/linux/local/vmware_mount	2013-08-22	excellent	VMWare Workstation (up to an build-1031769) and Player hav executable called vmware-mou lsb_release in the PATH with pc PATH is user-controlled, ... **Platforms**: linux **CVEs**: CVE-2013-1662 **Refs**: source, ref1, ref2, ref3
Yum Package Manager Persistence exploit/linux/local/yum_package_manager_persistence	2003-12-17	excellent	This module will run a payload package manager is used. No l automatically so you must conf appropriate exploit/multi/handle Module modifies a yum plugin t **Platforms**: linux, unix **Refs**: source, ref1
ZPanel zsudo Local Privilege Escalation Exploit exploit/linux/local/zpanel_zsudo	2013-06-07	excellent	This module abuses the zsudo with zpanel, to escalate privileg work, a session with access to sudoers configuration is neede useful for ... **Platforms**: linux, unix **Refs**: source
Borland InterBase open_marker_file() Buffer Overflow exploit/linux/misc/ib_open_marker_file	2007-10-03	good	This module exploits a stack bu Borland InterBase by sending a attach request. **Platforms**: linux **CVEs**: CVE-2007-5244 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Accellion FTA MPIPE2 Command Execution exploit/linux/misc/accellion_fta_mpipe2	2011-02-07	excellent	This module exploits a chain of the Accellion File Transfer appl appliance exposes a UDP serv that acts as a gateway to the in communication bus. ... **Platforms**: unix **Refs**: source, ref1
Aerospike Database UDF Lua Code Execution exploit/linux/misc/aerospike_database_udf_cmd_exec	2020-07-31	great	Aerospike Database versions b permitted user-defined function the `os.execute` Lua function. T creates a UDF utilising this fun arbitrary ... **Platforms**: linux, unix **CVEs**: CVE-2020-13151 **Refs**: source, ref1, ref2, ref3, re
ASUS infosvr Auth Bypass Command Execution exploit/linux/misc/asus_infosvr_auth_bypass_exec	2015-01-04	excellent	This module exploits an authen vulnerability in the infosvr servi UDP port 9999 on various ASU execute arbitrary commands as module launches the ... **Platforms**: unix **CVEs**: CVE-2014-9583 **Refs**: source, ref1
AnyDesk GUI Format String Write exploit/linux/misc/cve_2020_13160_anydesk	2020-06-16	normal	The AnyDesk GUI is vulnerable exploitable format string vulner sending a specially crafted disc attacker can corrupt the fronter it loads or ... **Platforms**: linux **CVEs**: CVE-2020-13160 **Refs**: source, ref1
GLD (Greylisting Daemon) Postfix Buffer Overflow exploit/linux/misc/gld_postfix	2005-04-12	good	This module exploits a stack bu the Salim Gasmi GLD <= 1.4 g daemon for Postfix. By sending string the stack can be overwrit **Platforms**: linux **CVEs**: CVE-2005-1099 **Refs**: source
HID discoveryd command_blink_on Unauthenticated RCE exploit/linux/misc/hid_discoveryd_command_blink_on_unauth_rce	2016-03-28	excellent	This module exploits an unauth command execution vulnerabili discoveryd service exposed by Edge door controllers. This mo successfully on a HID ... **Platforms**: linux **Refs**: source, ref1, ref2, ref3, re
Hikvision DVR RTSP Request Remote Code Execution exploit/linux/misc/hikvision_rtsp_bof	2014-11-19	normal	This module exploits a buffer o RTSP request parsing code of appliances. The Hikvision DVR video feeds of surveillance cam remote ... **Platforms**: linux **CVEs**: CVE-2014-4880 **Refs**: source, ref1
HPLIP hpssd.py From Address Arbitrary Command Execution exploit/linux/misc/hplip_hpssd_exec	2007-10-04	excellent	This module exploits a comma vulnerable in the hpssd.py daer Hewlett-Packard Linux Imaging Project. According to MITRE, v 2.x before 2.7.10 are ... **Platforms**: unix **CVEs**: CVE-2007-5208 **Refs**: source, ref1, ref2
HP Data Protector 6 EXEC_CMD Remote Code Execution exploit/linux/misc/hp_data_protector_cmd_exec	2011-02-07	excellent	This exploit abuses a vulnerabi Data Protector service. This fla unauthenticated attacker to tak the EXEC_CMD command and /bin/sh, this allows ... **Platforms**: linux, unix **CVEs**: CVE-2011-0923 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
HP Jetdirect Path Traversal Arbitrary Code Execution exploit/linux/misc/hp_jetdirect_path_traversal	2017-04-05	normal	The module exploits a path trav Jetdirect to gain arbitrary code writing a shell script that is load /etc/profile.d. Then, the printer SNMP. ... **Platforms**: unix **CVEs**: CVE-2017-2741 **Refs**: source, ref1, ref2
HP Network Node Manager I PMD Buffer Overflow exploit/linux/misc/hp_nnmi_pmd_bof	2014-09-09	normal	This module exploits a stack bu HP Network Node Manager I (N vulnerability exists in the pmd s the insecure usage of functions strcat while ... **Platforms**: unix **CVEs**: CVE-2014-2624 **Refs**: source
HP StorageWorks P4000 Virtual SAN Appliance Login Buffer Overflow exploit/linux/misc/hp_vsa_login_bof	2013-06-28	normal	This module exploits a buffer ov vulnerability found in HP's Stora VSA on versions prior to 10.0. T is due to an insecure usage of t function when ... **Platforms**: linux **CVEs**: CVE-2013-2343 **Refs**: source, ref1
Borland InterBase INET_connect() Buffer Overflow exploit/linux/misc/ib_inet_connect	2007-10-03	good	This module exploits a stack bu Borland InterBase by sending a service attach request. **Platforms**: linux **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Borland InterBase jrd8_create_database() Buffer Overflow exploit/linux/misc/ib_jrd8_create_database	2007-10-03	good	This module exploits a stack bu Borland InterBase by sending a create request. **Platforms**: linux **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Borland InterBase PWD_db_aliased() Buffer Overflow exploit/linux/misc/ib_pwd_db_aliased	2007-10-03	good	This module exploits a stack bu Borland InterBase by sending a attach request. **Platforms**: linux **CVEs**: CVE-2007-5243 **Refs**: source, ref1
Jenkins CLI RMI Java Deserialization Vulnerability exploit/linux/misc/jenkins_java_deserialize	2015-11-18	excellent	This module exploits a vulnerab An unsafe deserialization bug e Jenkins master, which allows re code execution. Authentication exploit ... **Platforms**: java **CVEs**: CVE-2015-8103 **Refs**: source, ref1, ref2, ref3, re
Jenkins CLI HTTP Java Deserialization Vulnerability exploit/linux/misc/jenkins_ldap_deserialize	2016-11-16	excellent	This module exploits a vulnerab An unsafe deserialization bug e Jenkins, which allows remote a execution via HTTP. Authentica required to exploit ... **Platforms**: linux, unix **CVEs**: CVE-2016-9299 **Refs**: source, ref1, ref2, ref3, re
LPRng use_syslog Remote Format String Vulnerability exploit/linux/misc/lprng_format_string	2000-09-25	normal	This module exploits a format s in the LPRng print server. This discovered by Chris Evans. The publicly circulating worm target vulnerability, ... **Platforms**: linux **CVEs**: CVE-2000-0917 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
MongoDB nativeHelper.apply Remote Code Execution exploit/linux/misc/mongod_native_helper	2013-03-24	normal	This module exploits the native from spiderMonkey which allow execution by calling it with spec arguments. This module has be successfully on MongoDB ... **Platforms**: linux **CVEs**: CVE-2013-1892 **Refs**: source, ref1
Nagios Remote Plugin Executor Arbitrary Command Execution exploit/linux/misc/nagios_nrpe_arguments	2013-02-21	excellent	The Nagios Remote Plugin Exe installed to allow a central Nagi actively poll information from th monitors. NRPE has a configur dont_blame_nrpe which ... **Platforms**: unix **CVEs**: CVE-2013-1362 **Refs**: source, ref1
Netcore Router Udp 53413 Backdoor exploit/linux/misc/netcore_udp_53413_backdoor	2014-08-25	normal	Routers manufactured by Netc brand for networking equipmen a wide-open backdoor that can exploited by attackers. These p sold under the ... **Platforms**: linux **Refs**: source, ref1, ref2, ref3
NetSupport Manager Agent Remote Buffer Overflow exploit/linux/misc/netsupport_manager_agent	2011-01-08	average	This module exploits a buffer o NetSupport Manager Agent. It ROP to the proftpd_iac exploit non executable stack. **Platforms**: linux **CVEs**: CVE-2011-0404 **Refs**: source, ref1
Novell eDirectory 8 Buffer Overflow exploit/linux/misc/novell_edirectory_ncp_bof	2012-12-12	normal	This exploit abuses a buffer ov vulnerability in Novell eDirector vulnerability exists in the ndsd specifically in the NCP service, specially crafted Keyed Object **Platforms**: linux **CVEs**: CVE-2012-0432 **Refs**: source, ref1, ref2
OpenNMS Java Object Unserialization Remote Code Execution exploit/linux/misc/opennms_java_serialize	2015-11-06	normal	This module exploits a vulneral OpenNMS Java object which a unauthenticated attacker to run against the system. **Platforms**: linux **CVEs**: CVE-2015-8103 **Refs**: source, ref1
QNAP Transcode Server Command Execution exploit/linux/misc/qnap_transcode_server	2017-08-06	excellent	This module exploits an unauth command injection vulnerability devices. The transcoding serve 9251 by default and is vulnerab injection using ... **Platforms**: linux **CVEs**: CVE-2017-13067 **Refs**: source, ref1, ref2
Quest Privilege Manager pmmasterd Buffer Overflow exploit/linux/misc/quest_pmmasterd_bof	2017-04-09	normal	This modules exploits a buffer Quest Privilege Manager, a sof integrate Active Directory with systems. The vulnerability exist pmmasterd daemon, ... **Platforms**: unix **CVEs**: CVE-2017-6553, CVE-2 **Refs**: source, ref1
SaltStack Salt Master/Minion Unauthenticated RCE exploit/linux/misc/saltstack_salt_unauth_rce	2020-04-30	great	This module exploits unauthent the runner() and _send_pub() r SaltStack Salt master's ZeroM for versions 2019.2.3 and earlie and earlier, to ... **Platforms**: python, unix **CVEs**: CVE-2020-11651, CVE- **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
SerComm Device Remote Code Execution exploit/linux/misc/sercomm_exec	2013-12-31	great	This module will cause remote on several SerComm devices. typically include routers from N Linksys. This module was teste against several NetGear, ... **Platforms**: linux **Refs**: source, ref1
TP-Link Archer A7/C7 Unauthenticated LAN Remote Code Execution exploit/linux/misc/tplink_archer_a7_c7_lan_rce	2020-03-25	excellent	This module exploits a commar vulnerability in the tdpServer da (/usr/bin/tdpServer), running on Link Archer A7/C7 (AC1750), h 5, MIPS Architecture, ... **Platforms**: linux **CVEs**: CVE-2020-10882, CVE- CVE-2020-10884, CVE-2020-2 **Refs**: source, ref1, ref2, ref3, re
Unitrends UEB bpserverd authentication bypass RCE exploit/linux/misc/ueb9_bpserverd	2017-08-08	excellent	It was discovered that the Unitr proprietary protocol, as expose an issue in which its authentica bypassed. A remote attacker cc issue to execute ... **Platforms**: linux **CVEs**: CVE-2017-12477 **Refs**: source, ref1, ref2
Zabbix Server Arbitrary Command Execution exploit/linux/misc/zabbix_server_exec	2009-09-10	excellent	This module abuses the "Comr Zabbix Server to execute arbitr without authentication. By defa "0" is used, if it doesn't work, th leaked from the ... **Platforms**: unix **CVEs**: CVE-2009-4498 **Refs**: source, ref1
MySQL yaSSL CertDecoder::GetName Buffer Overflow exploit/linux/mysql/mysql_yassl_getname	2010-01-25	good	This module exploits a stack bu the yaSSL (1.9.8 and earlier) in bundled with MySQL. By sendi crafted client certificate, an atta arbitrary ... **Platforms**: linux **CVEs**: CVE-2009-4484 **Refs**: source, ref1
MySQL yaSSL SSL Hello Message Buffer Overflow exploit/linux/mysql/mysql_yassl_hello	2008-01-04	good	This module exploits a stack bu the yaSSL (1.7.5 and earlier) in bundled with MySQL <= 6.0. By specially crafted Hello packet, a be able to execute ... **Platforms**: linux **CVEs**: CVE-2008-0226 **Refs**: source
Cyrus IMAPD pop3d popsubfolders USER Buffer Overflow exploit/linux/pop3/cyrus_pop3d_popsubfolders	2006-05-21	normal	This exploit takes advantage of overflow. Once the stack corrup occurred it is possible to overw which is later used for a memcp a write anything ... **Platforms**: linux **CVEs**: CVE-2006-2502 **Refs**: source, ref1
PostgreSQL for Linux Payload Execution exploit/linux/postgres/postgres_payload	2007-06-05	excellent	On some default Linux installat PostgreSQL, the postgres serv write to the /tmp directory, and Shared Libraries from there as execution of ... **Platforms**: linux **CVEs**: CVE-2007-3280 **Refs**: source, ref1
Poptop Negative Read Overflow exploit/linux/pptp/poptop_negative_read	2003-04-09	great	This is an exploit for the Poptop overflow. This will work against 1.1.3-b3 and 1.1.3-20030409, b not have a good way to detect The ... **Platforms**: linux **CVEs**: CVE-2003-0213 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Squid NTLM Authenticate Overflow exploit/linux/proxy/squid_ntlm_authenticate	2004-06-08	great	This is an exploit for Squid's NT overflow (libntlmssp.c). Due to checking in ntlm_check_auth, it overflow the 'pass' variable on t user ... **Platforms**: linux **CVEs**: CVE-2004-0541 **Refs**: source, ref1
Redis Replication Code Execution exploit/linux/redis/redis_replication_cmd_exec	2018-11-13	good	This module can be used to lev extension functionality added s to execute arbitrary code. To tr extension it makes use of the fe which called ... **Platforms**: linux **Refs**: source, ref1, ref2
Samba chain_reply Memory Corruption (Linux x86) exploit/linux/samba/chain_reply	2010-06-16	good	This exploits a memory corrupt present in Samba versions prio When handling chained respon Samba fails to validate the offs when building the next ... **Platforms**: linux **CVEs**: CVE-2010-2063 **Refs**: source, ref1
Samba is_known_pipename() Arbitrary Module Load exploit/linux/samba/is_known_pipename	2017-03-24	excellent	This module triggers an arbitrar load vulnerability in Samba ver 4.4.14, 4.5.10, and 4.6.4. This r valid credentials, a writeable fo accessible ... **Platforms**: linux, unix **CVEs**: CVE-2017-7494 **Refs**: source, ref1
Samba lsa_io_trans_names Heap Overflow exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	This module triggers a heap ov RPC service of the Samba dae module uses the TALLOC chur method (credit Ramon and Adr works with Samba versions ... **Platforms**: linux **CVEs**: CVE-2007-2446 **Refs**: source
Samba SetInformationPolicy AuditEventsInfo Heap Overflow exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	This module triggers a vulnerab RPC service of the Samba dae an error on the PIDL auto-gene Making a specially crafted call t SetInformationPolicy to set a .. **Platforms**: linux, unix **CVEs**: CVE-2012-1182 **Refs**: source
Samba trans2open Overflow (Linux x86) exploit/linux/samba/trans2open	2003-04-07	great	This exploits the buffer overflov versions 2.2.0 to 2.2.8. This pa capable of exploiting the flaw o systems that do not have the n option set. ... **Platforms**: linux **CVEs**: CVE-2003-0201 **Refs**: source, ref1
Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write exploit/linux/smtp/apache_james_exec	2015-10-01	normal	This module exploits a vulnerab due to a lack of input validation user. Messages for a given use directory partially defined by th ... **Platforms**: linux **CVEs**: CVE-2015-7611 **Refs**: source, ref1
Exim and Dovecot Insecure Configuration Command Injection exploit/linux/smtp/exim4_dovecot_exec	2013-05-03	excellent	This module exploits a commar vulnerability against Dovecot w the "use_shell" option. It uses t address to inject arbitrary comr is one of the ... **Platforms**: linux **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Exim GHOST (glibc gethostbyname) Buffer Overflow exploit/linux/smtp/exim_gethostbyname_bof	2015-01-27	great	This module remotely exploits (aka GHOST, a heap-based buf the GNU C Library's gethostby on x86 and x86_64 GNU/Linux the Exim mail server. **Platforms**: linux, unix **CVEs**: CVE-2015-0235 **Refs**: source, ref1, ref2, ref3
AwindInc SNMP Service Command Injection exploit/linux/snmp/awind_snmp_exec	2019-03-27	excellent	This module exploits a vulneral AwindInc and OEM'ed product inputs are fed to ftpfw.sh syste leading to command injection. A read-write community ... **Platforms**: linux, unix **CVEs**: CVE-2017-16709 **Refs**: source, ref1, ref2
Net-SNMPd Write Access SNMP-EXTEND-MIB arbitrary code execution exploit/linux/snmp/net_snmpd_rw_access	2004-05-10	normal	This exploit module exploits the access configuration ability of S MIB to configure MIB extensio remote code execution. **Platforms**: linux **Refs**: source, ref1, ref2, ref3, re
Ceragon FibeAir IP-10 SSH Private Key Exposure exploit/linux/ssh/ceragon_fibeair_known_privkey	2015-04-01	excellent	Ceragon ships a public/private FibeAir IP-10 devices that allo authentication to any other IP-1 the key is easily retrievable, an it to gain ... **Platforms**: unix **CVEs**: CVE-2015-0936 **Refs**: source, ref1
Cisco UCS Director default scpuser password exploit/linux/ssh/cisco_ucs_scpuser	2019-08-21	excellent	This module abuses a known d on Cisco UCS Director. The 'sc password of 'scpuser', and allo login to the virtual appliance via module has been ... **Platforms**: unix **CVEs**: CVE-2019-1935 **Refs**: source, ref1, ref2, ref3
ExaGrid Known SSH Key and Default Password exploit/linux/ssh/exagrid_known_privkey	2016-04-07	excellent	ExaGrid ships a public/private k backup appliances to allow pas authentication to other ExaGrid Since the private key is easily r attacker can use ... **Platforms**: unix **CVEs**: CVE-2016-1560, CVE-2 **Refs**: source, ref1
F5 BIG-IP SSH Private Key Exposure exploit/linux/ssh/f5_bigip_known_privkey	2012-06-11	excellent	F5 ships a public/private key pa appliances that allows passwor authentication to any other BIG the key is easily retrievable, an it to gain ... **Platforms**: unix **CVEs**: CVE-2012-1493 **Refs**: source, ref1, ref2
IBM Data Risk Manager a3user Default Password exploit/linux/ssh/ibm_drm_a3user	2020-04-21	excellent	This module abuses a known d in IBM Data Risk Manager. The default password 'idrm' and allo to log in to the virtual appliance can be ... **Platforms**: unix **CVEs**: CVE-2020-4427, CVE-2 2020-4429, CVE-2020-4430 **Refs**: source, ref1, ref2, ref3
Loadbalancer.org Enterprise VA SSH Private Key Exposure exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey	2014-03-17	excellent	Loadbalancer.org ships a publi on Enterprise virtual appliances that allows passwordless authe other LB Enterprise box. Since ... **Platforms**: unix **Refs**: source

Metasploit Module	Date	Rank	Details
Mercurial Custom hg-ssh Wrapper Remote Code Exec exploit/linux/ssh/mercurial_ssh_exec	2017-04-18	excellent	This module takes advantage c wrapper implementations that c validate parameters passed to allowing users to trigger a Pyth session, which ... **Platforms**: python **CVEs**: CVE-2017-9462 **Refs**: source, ref1
Quantum DXi V1000 SSH Private Key Exposure exploit/linux/ssh/quantum_dxi_known_privkey	2014-03-17	excellent	Quantum ships a public/private V1000 2.2.1 appliances that all passwordless authentication to box. Since the key is easily retr attacker can use it to gain ... **Platforms**: unix **Refs**: source
Quantum vmPRO Backdoor Command exploit/linux/ssh/quantum_vmpro_backdoor	2014-03-17	excellent	This module abuses a backdoc Quantum vmPRO. Any user, ev admin privileges, can get acces restricted SSH shell. By using t backdoor "shell-escape" comm **Platforms**: unix **Refs**: source
SolarWinds LEM Default SSH Password Remote Code Execution exploit/linux/ssh/solarwinds_lem_exec	2017-03-17	excellent	This module exploits the defaul SolarWinds LEM. A menu syste encountered when the SSH ser with the default username and is "cmc" and "password". By ... **Platforms**: python **CVEs**: CVE-2017-7722 **Refs**: source, ref1
Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability exploit/linux/ssh/symantec_smg_ssh	2012-08-27	excellent	This module exploits a default r flaw on Symantec Messaging G 'support' user has a known defa which can be used to login to th and gain privileged ... **Platforms**: unix **CVEs**: CVE-2012-3579 **Refs**: source, ref1
VMware VDP Known SSH Key exploit/linux/ssh/vmware_vdp_known_privkey	2016-12-20	excellent	VMware vSphere Data Protecti 5.5.x through 6.1.x contain a kr key for the local user admin wh without password. **Platforms**: unix **CVEs**: CVE-2016-7456 **Refs**: source, ref1
VyOS restricted-shell Escape and Privilege Escalation exploit/linux/ssh/vyos_restricted_shell_privesc	2018-11-05	great	This module exploits command vulnerabilities and an insecure configuration on VyOS versions to execute arbitrary system cor VyOS features a ... **Platforms**: unix **CVEs**: CVE-2018-18556 **Refs**: source, ref1, ref2, ref3
NETGEAR TelnetEnable exploit/linux/telnet/netgear_telnetenable	2009-10-30	excellent	This module sends a magic pa NETGEAR device to enable tel successful connect, a root shel presented to the user. **Platforms**: unix **Refs**: source, ref1, ref2, ref3
Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow exploit/linux/telnet/telnet_encrypt_keyid	2011-12-23	great	This module exploits a buffer o encryption option handler of the derived telnet service (inetutils Most Linux distributions use Ne telnet daemons, ... **Platforms**: linux **CVEs**: CVE-2011-4862 **Refs**: source

Metasploit Module	Date	Rank	Details
Belkin Wemo UPnP Remote Code Execution exploit/linux/upnp/belkin_wemo_upnp_exec	2014-04-04	excellent	This module exploits a commar Belkin Wemo UPnP API via the argument to the SetSmartDevIr module has been tested on a V Crock-Pot, but other ... **Platforms**: linux, unix **Refs**: source, ref1, ref2, ref3, re ref7
D-Link Devices Unauthenticated Remote Command Execution in ssdpcgi exploit/linux/upnp/dlink_dir859_exec_ssdpcgi	2019-12-24	excellent	D-Link Devices Unauthenticate Command Execution in ssdpcg **Platforms**: linux **CVEs**: CVE-2019-20215 **Refs**: source, ref1
D-Link DIR-859 Unauthenticated Remote Command Execution exploit/linux/upnp/dlink_dir859_subscribe_exec	2019-12-24	excellent	D-Link DIR-859 Routers are vu command injection via the UPn vulnerability exists in /gena.cgi genacgi_main() in /htdocs/cgibi accessible without ... **Platforms**: linux **CVEs**: CVE-2019-17621 **Refs**: source, ref1
D-Link Unauthenticated UPnP M-SEARCH Multicast Command Injection exploit/linux/upnp/dlink_upnp_msearch_exec	2013-02-01	excellent	Different D-Link Routers are vu command injection via UPnP M This module has been tested o DIR-645 devices. Zachary Cutl reported the ... **Platforms**: linux **Refs**: source, ref1, ref2
MiniUPnPd 1.0 Stack Buffer Overflow Remote Code Execution exploit/linux/upnp/miniupnpd_soap_bof	2013-03-27	normal	This module exploits the MiniU stack buffer overflow vulnerabil SOAPAction HTTP header han **Platforms**: linux **CVEs**: CVE-2013-0230 **Refs**: source, ref1
Firefox PDF.js Privileged Javascript Injection exploit/multi/browser/firefox_pdfjs_privilege_escalation	2015-03-31	manual	This module gains remote code Firefox 35-36 by abusing a priv bug in resource:// URIs. PDF.js the bug. This exploit requires th anywhere ... **Platforms**: firefox, java, linux, c **CVEs**: CVE-2015-0802, CVE-2 **Refs**: source
Java Applet JAX-WS Remote Code Execution exploit/multi/browser/java_jre17_jaxws	2012-10-16	excellent	This module abuses the JAX-W Java Applet to run arbitrary Jav of the sandbox as exploited in t November of 2012. The vulnera Java version 7u7 and ... **Platforms**: java, linux, win **CVEs**: CVE-2012-5067, CVE-2 **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 aft Flash Player. The vulnerability, Hacking Team and made public July 2015 data leak, was descr 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 o Flash Player when handling ne encoded audio inside a FLV vic in the wild on June 2015. This r tested successfully ... **Platforms**: linux, win **CVEs**: CVE-2015-3043, CVE-2 **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
Adobe Flash Player NetConnection Type Confusion exploit/multi/browser/adobe_flash_net_connection_confusion	2015-03-12	great	This module exploits a type cor vulnerability in the NetConnecti Adobe Flash Player. When usir memory layout this vulnerability corrupt arbitrary memory. It car **Platforms**: linux, win **CVEs**: CVE-2015-0336 **Refs**: source, ref1, ref2, ref3, re
Adobe Flash Player Shader Buffer Overflow exploit/multi/browser/adobe_flash_pixel_bender_bof	2014-04-28	great	This module exploits a buffer o vulnerability in Adobe Flash Pla vulnerability occurs in the flash class, when setting specially cr bytecode, as ... **Platforms**: linux, win **CVEs**: CVE-2014-0515 **Refs**: source, ref1, ref2, ref3
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 happening when applying a Sh drawing fill as exploited in the v 2015. This module has been te on: Windows 7 SP1 (32-bit), ... **Platforms**: linux, win **CVEs**: CVE-2015-3105 **Refs**: source, ref1, ref2, ref3, re
Adobe Flash Player ShaderJob Buffer Overflow exploit/multi/browser/adobe_flash_shader_job_overflow	2015-05-12	great	This module exploits a buffer o vulnerability related to the Shac on Adobe Flash Player. The vu happens when trying to apply a up the same Bitmap object ... **Platforms**: linux, win **CVEs**: CVE-2015-3090 **Refs**: source, ref1, ref2, ref3, re
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 afte vulnerability in Adobe Flash Pla vulnerability occurs in the ByteArray::UncompressViaZlib' when trying to uncompress() a ... **Platforms**: linux, win **CVEs**: CVE-2015-0311 **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 co Google Chromes JIT compiler. Object.create operation can be type confusion between a Prop NameDictionary. The payload is **Platforms**: linux, osx, win **CVEs**: CVE-2018-17463, CVE- **Refs**: source, ref1, ref2, ref3, re
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 i Chrome versions before 87.0.4 The exploit makes use of a inte the SimplifiedLowering phase ir used along with a ... **Platforms**: linux, osx, win **CVEs**: CVE-2020-16040 **Refs**: source, ref1, ref2, ref3, re
Firefox Proxy Prototype Privileged Javascript Injection exploit/multi/browser/firefox_proxy_prototype	2014-01-20	manual	This exploit gains remote code Firefox 31-34 by abusing a bug XPConnect component and ga to the privileged chrome:// wind requires the user to ... **Platforms**: firefox, java, linux, c **CVEs**: CVE-2014-8636, CVE-2 **Refs**: source, ref1, ref2
Firefox location.QueryInterface() Code Execution exploit/multi/browser/firefox_queryinterface	2006-02-02	normal	This module exploits a code ex vulnerability in the Mozilla Firef reliably exploit this vulnerability almost a gigabyte of memory w and payload. ... **Platforms**: linux, osx **CVEs**: CVE-2006-0295 **Refs**: source, ref1

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 Firefox 17 and 17.0.1, provided installed Flash. No memory cor First, a Flash object is cloned ir anonymous content of ... **Platforms**: firefox, java, linux, c **CVEs**: CVE-2013-0757, CVE-2 **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 Firefox 15-22 by abusing two s Javascript-related vulnerabilitie inject malicious Javascript code running with ... **Platforms**: firefox, java, linux, c **CVEs**: CVE-2013-1670, CVE-2 **Refs**: source
Firefox WebIDL Privileged Javascript Injection exploit/multi/browser/firefox_webidl_injection	2014-03-17	excellent	This exploit gains remote code Firefox 22-27 by abusing two s escalation vulnerabilities in Fire APIs. **Platforms**: firefox, java, linux, c **CVEs**: CVE-2014-1510, CVE-2 **Refs**: source
Java AtomicReferenceArray Type Violation Vulnerability exploit/multi/browser/java_atomicreferencearray	2012-02-14	excellent	This module exploits a vulneral fact that AtomicReferenceArray class to store a reference in an which may violate type safety if properly. ... **Platforms**: java, linux, osx, sola **CVEs**: CVE-2012-0507 **Refs**: source, ref1, ref2, ref3, re
Sun Java Calendar Deserialization Privilege Escalation exploit/multi/browser/java_calendar_deserialize	2008-12-03	excellent	This module exploits a flaw in t of Calendar objects in the Sun payload can be either a native generated as an executable an dropped/executed on the ... **Platforms**: java, linux, osx, sola **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 t getSoundbank function in the S payload is serialized and passe via PARAM tags. It must be a n 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.sc class where the toString() meth user supplied classes from a dc The vulnerability affects Java v ... **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 JDK 7: The ClassFinder and MethodFinder.findMethod(). Bo introduced in JDK 7. ClassFind replacement for classForName ... **Platforms**: java, linux, win **CVEs**: CVE-2012-4681 **Refs**: source, ref1, ref2, ref3, re ref7
Java Applet AverageRangeStatisticImpl Remote Code Execution exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl	2012-10-16	excellent	This module abuses the AverageRangeStatisticImpl fror to run arbitrary Java code outsi sandbox, a different exploit vec exploited in the wild in Novemb **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 c Java Applet to run arbitrary Jav of the sandbox as exploited in t January of 2013. The vulnerabi 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 c Java Applet to run arbitrary Jav of the sandbox as exploited in t February of 2013. Additionally, bypasses default ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-0431 **Refs**: source, ref1, ref2, ref3, re
Java Applet Method Handle Remote Code Execution exploit/multi/browser/java_jre17_method_handle	2012-10-16	excellent	This module abuses the Metho from a Java Applet to run arbitr outside of the sandbox. The vu 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 insecu method of the ProviderSkeletor allows to call arbitrary static me supplied arguments. The vulne Java version 7u21 ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-2460 **Refs**: source, ref1, ref2, ref3, re
Java Applet Reflection Type Confusion Remote Code Execution exploit/multi/browser/java_jre17_reflection_types	2013-01-10	excellent	This module abuses Java Refle a Type Confusion, due to a wea when setting final fields on stat run code outside of the Java Sa vulnerability ... **Platforms**: java, linux, osx, win **CVEs**: CVE-2013-2423 **Refs**: source, ref1, ref2, ref3, re
Java Applet Rhino Script Engine Remote Code Execution exploit/multi/browser/java_rhino	2011-10-18	excellent	This module exploits a vulnerat Script Engine that can be used to run arbitrary Java code outsi sandbox. The vulnerability affe 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 t function in the Sun JVM. The p serialized and passed to the ap tags. It must be a native payloa 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 create Msf::Exploit::Java mixin, then s resulting signed applet is prese via a web page with an applet t **Platforms**: java, linux, osx, sol **Refs**: source, ref1
Java storeImageArray() Invalid Array Indexing Vulnerability exploit/multi/browser/java_storeimagearray	2013-08-12	great	This module abuses an Invalid Vulnerability on the static functi storeImageArray() function in o memory corruption and escape 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 vulnerat Runtime Environment that allov method to run in a privileged cc vulnerability affects version 6 p 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 vulnerat bytecode verifier where an inva of GETFIELD/PUTFIELD/GETST/ instructions leads to insufficient This allows a ... **Platforms**: java, linux, osx, sol **CVEs**: CVE-2012-1723 **Refs**: source, ref1, ref2, ref3, re
Mozilla Suite/Firefox Navigator Object Code Execution exploit/multi/browser/mozilla_navigatorjava	2006-07-25	normal	This module exploits a code ex vulnerability in the Mozilla Suite and Mozilla Thunderbird applic exploit requires the Java plugin **Platforms**: linux, osx, win **CVEs**: CVE-2006-3677 **Refs**: source, ref1
Adobe U3D CLODProgressiveMeshDeclaration Array Overrun exploit/multi/fileformat/adobe_u3d_meshcont	2009-10-13	good	This module exploits an array c Reader and Adobe Acrobat. Af include < 7.1.4, < 8.1.7, and < 9 specially crafted pdf that a cont 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 -dSAFE Ghostscript to execute arbitrary handling a failed restore (grest to disable LockSafetyParams a 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 written in Python and allows the program events to them. A mac a program event by including th 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 files and execute commands au when opening a Maplet. All ver are suspected vulnerable. Testi conducted with version 13 ... **Platforms**: linux, unix, win **Refs**: source, ref1
PeaZip Zip Processing Command Injection exploit/multi/fileformat/peazip_command_injection	2009-06-05	excellent	This module exploits a commar vulnerability in PeaZip. All vers are suspected vulnerable. Testi conducted with version 2.6.1 or 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 o technique, which typically resul command execution. This targe widespread vulnerability that ha affecting a variety of ... **Platforms**: linux, unix, win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock) exploit/multi/ftp/pureftpd_bash_env_exec	2014-09-24	excellent	This module exploits the Shells vulnerability, a flaw in how the E handles external environment v module targets the Pure-FTPd it has been compiled with the .. **Platforms**: linux **CVEs**: CVE-2014-6271 **Refs**: source, ref1, ref2
WU-FTPD SITE EXEC/INDEX Format String Vulnerability exploit/multi/ftp/wuftpd_site_exec_format	2000-06-22	great	This module exploits a format s in versions of the Washington U server older than 2.6.1. By exe crafted SITE EXEC or SITE INI containing ... **Platforms**: linux **CVEs**: CVE-2000-0573 **Refs**: source
GDB Server Remote Payload Execution exploit/multi/gdb/gdb_server_exec	2014-08-24	great	This module attempts to execut payload on a loose gdbserver s **Platforms**: linux, osx, unix **Refs**: source, ref1
Steamed Hams exploit/multi/hams/steamed	2018-04-01	manual	but it's a Metasploit Module. **Platforms**: android, apple_ios, linux, mainframe, multi, nodejs, python, ruby, solaris, unix, win **Refs**: source, ref1
Generic Payload Handler exploit/multi/handler	-	manual	This module is a stub that prov features of the Metasploit payl exploits that have been launche framework. **Platforms**: android, apple_ios, linux, mainframe, multi, nodejs, python, ruby, solaris, unix, win **Refs**: source
Agent Tesla Panel Remote Code Execution exploit/multi/http/agent_tesla_panel_rce	2019-08-14	excellent	This module exploits a commar vulnerability within the Agent Te panel, in combination with an S vulnerability and a PHP object 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 arbitra execution vulnerability in the Aj 'checkInstall.php' script. All vers AjaXplorer prior to 2.6 are vuln **Platforms**: bsd, linux, osx, unix **Refs**: source
ActiveMQ web shell upload exploit/multi/http/apache_activemq_upload_jsp	2016-06-01	excellent	The Fileserver web application ActiveMQ 5.x before 5.14.0 allc attackers to upload and execut via an HTTP PUT followed by a request. **Platforms**: java, linux, win **CVEs**: CVE-2016-3088 **Refs**: source, ref1
Apache Jetspeed Arbitrary File Upload exploit/multi/http/apache_jetspeed_file_upload	2016-03-06	manual	This module exploits the unsec Manager REST API and a ZIP in Apache Jetspeed-2, version unknown earlier versions, to up execute a shell. Note: this ... **Platforms**: linux, win **CVEs**: CVE-2016-0709, CVE-2 **Refs**: source, ref1, ref2, ref3
Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) exploit/multi/http/apache_mod_cgi_bash_env_exec	2014-09-24	excellent	This module exploits the Shells vulnerability, a flaw in how the E handles external environment v module targets CGI scripts in th server by setting the ... **Platforms**: linux **CVEs**: CVE-2014-6271, CVE-2 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Apache NiFi API Remote Code Execution exploit/multi/http/apache_nifi_processor_rce	2020-10-03	excellent	This module uses the NiFi API ExecuteProcess processor that commands. The API must be u credentials provided) and the E 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 arbitra vulnerability together with a dire flaw in ATutor versions 2.2.4, 2 order to execute arbitrary comr creates ... **Platforms**: linux, win **CVEs**: CVE-2019-12169 **Refs**: source, ref1
Auxilium RateMyPet Arbitrary File Upload Vulnerability exploit/multi/http/auxilium_upload_exec	2012-09-14	excellent	This module exploits a vulnerat Auxilium RateMyPet's. The site uploading feature can be abuse arbitrary file to the web server, accessible in the 'banner' ... **Platforms**: linux, php **Refs**: source
Axis2 / SAP BusinessObjects Authenticated Code Execution (via SOAP) exploit/multi/http/axis2_deployer	2010-12-30	excellent	This module logs in to an Axis2 Module instance using a specif uploads and executes comman a malicious web service by usir **Platforms**: java, linux, win **CVEs**: CVE-2010-0219 **Refs**: source, ref1, ref2
Bassmaster Batch Arbitrary JavaScript Injection Remote Code Execution exploit/multi/http/bassmaster_js_injection	2016-11-01	excellent	This module exploits an un-aut injection vulnerability in the bas plugin for hapi. The vulnerabilit batch endpoint and allows an a dynamically ... **Platforms**: bsd, linux **CVEs**: CVE-2014-7205 **Refs**: source, ref1
Cisco Data Center Network Manager Unauthenticated Remote Code Execution exploit/multi/http/cisco_dcnm_upload_2019	2019-06-26	excellent	DCNM exposes a file upload se (FileUploadServlet) at /fm/fileU authenticated user can abuse t upload a WAR to the Apache T directory and achieve remote c **Platforms**: java **CVEs**: CVE-2019-1619, CVE-2019-1622 **Refs**: source, ref1, ref2, ref3, re
ClipBucket beats_uploader Unauthenticated Arbitrary File Upload exploit/multi/http/clipbucket_fileupload_exec	2018-03-03	excellent	This module exploits a vulnerat ClipBucket versions before 4.0 4902). A malicious file can be u an unauthenticated arbitrary file 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 Adobe ColdFusion 11 (Update ColdFusion 2016 (Update 6 an ColdFusion 2018 (July 12 relea 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 allows remote attackers to bypa authentication using the RDS c to default settings or misconfigu password can be set to an emp **Platforms**: linux, win **CVEs**: CVE-2013-0632 **Refs**: source

Metasploit Module	Date	Rank	Details
Atlassian Confluence Widget Connector Macro Velocity Template Injection exploit/multi/http/confluence_widget_connector	2019-03-25	excellent	Widget Connector Macro is par Confluence Server and Data C embed online videos, slideshov and more directly into page. A parameter can be used ... **Platforms**: java, linux, win **CVEs**: CVE-2019-3396 **Refs**: source, ref1, ref2, ref3
Network Shutdown Module (sort_values) Remote PHP Code Injection exploit/multi/http/eaton_nsm_code_exec	2012-06-26	excellent	This module exploits a vulneral Network Shutdown Module ver lib/dbtools.inc which uses unsa inside a eval() call. Additionally encoded user ... **Platforms**: linux, php **Refs**: source, ref1
ManageEngine Eventlog Analyzer Arbitrary File Upload exploit/multi/http/eventlog_file_upload	2014-08-31	excellent	This module exploits a file uplo ManageEngine Eventlog Analy vulnerability exists in the agent which accepts unauthenticated handles zip file ... **Platforms**: java, linux, win **CVEs**: CVE-2014-6037 **Refs**: source, ref1, ref2
Family Connections less.php Remote Command Execution exploit/multi/http/familycms_less_exec	2011-11-29	excellent	This module exploits an arbitra execution vulnerability in Famil 2.7.1. It's in the dev/less.php sc an insecure use of system(). Au required ... **Platforms**: linux, unix **CVEs**: CVE-2011-5130 **Refs**: source, ref1, ref2, ref3
Gitea Git Hooks Remote Code Execution exploit/multi/http/gitea_git_hooks_rce	2020-10-07	excellent	This module leverages an inse get remote code execution on t the context of the user running possible when the current user create `git ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-14144 **Refs**: source, ref1, ref2
Gitlab-shell Code Execution exploit/multi/http/gitlab_shell_exec	2013-11-04	excellent	This module takes advantage c authorized ssh keys in the gitla functionality of Gitlab. Versions prior to 1.7.4 used the ssh key in a system ... **Platforms**: linux, python, unix **CVEs**: CVE-2013-4490 **Refs**: source, ref1
Gitorious Arbitrary Command Execution exploit/multi/http/gitorious_graph	2012-01-19	excellent	This module exploits an arbitra execution vulnerability in gitoric input is passed to the shell allo execution. **Platforms**: linux, unix **Refs**: source, ref1
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 affects Git (versions less than 1 2.0.5, 2.1.4 and 2.2.1) and Mer less than 3.2.3) and describes vulnerabilities. On ... **Platforms**: unix, win **CVEs**: CVE-2014-9390 **Refs**: source, ref1, ref2, ref3, re ref7, ref8
Sun/Oracle GlassFish Server Authenticated Code Execution exploit/multi/http/glassfish_deployer	2011-08-04	excellent	This module logs in to a GlassF (Open Source or Commercial) methods (such as authenticatic credentials, or user-supplied lo a malicious war ... **Platforms**: java, linux, win **CVEs**: CVE-2011-0807 **Refs**: source

Metasploit Module	Date	Rank	Details
Gogs Git Hooks Remote Code Execution exploit/multi/http/gogs_git_hooks_rce	2020-10-07	excellent	This module leverages an inse get remote code execution on t the context of the user running possible when the current user create `git ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-14144, CVE- **Refs**: source, ref1, ref2
Horde 3.3.12 Backdoor Arbitrary PHP Code Execution exploit/multi/http/horde_href_backdoor	2012-02-13	excellent	This module exploits an arbitra execution vulnerability introduc into Horde 3.3.12 and Horde G **Platforms**: linux, unix **CVEs**: CVE-2012-0209 **Refs**: source, ref1, ref2
HorizontCMS Arbitrary PHP File Upload exploit/multi/http/horizontcms_upload_exec	2020-09-24	excellent	This module exploits an arbitra vulnerability in HorizontCMS 1. to execute arbitrary commands first attempts to authenticate to then tries ... **Platforms**: linux, php, win **CVEs**: CVE-2020-27387 **Refs**: source
HP SiteScope Remote Code Execution exploit/multi/http/hp_sitescope_uploadfileshandler	2012-08-29	good	This module exploits a code ex HP SiteScope. It exploits two v order to get its objective. An au bypass in the create operation, through the ... **Platforms**: linux, win **CVEs**: CVE-2012-3260, CVE-2 **Refs**: source
HP System Management Homepage JustGetSNMPQueue Command Injection exploit/multi/http/hp_sys_mgmt_exec	2013-06-11	excellent	This module exploits a vulnerat System Management Homepag a specially crafted HTTP reque to control the 'tempfilename' va ... **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 Groovy script console to execu using Java. Valid credentials fo administrator user account are module has been ... **Platforms**: linux, unix, vbs, win **Refs**: source, ref1
IBM OpenAdmin Tool SOAP welcomeServer PHP Code Execution exploit/multi/http/ibm_openadmin_tool_soap_welcomeserver_exec	2017-05-30	excellent	This module exploits an unauth PHP code execution vulnerabil OpenAdmin Tool included with versions 11.5, 11.7, and 12.1. T 'welcomeServer' SOAP service **Platforms**: php **CVEs**: CVE-2017-1092 **Refs**: source, ref1, ref2, ref3
Micro Focus Operations Bridge Manager Authenticated Remote Code Execution exploit/multi/http/microfocus_obm_auth_rce	2020-10-28	excellent	This module exploits an authen deserialization that affects a tru Focus products: Operations Bri Application Performance Mana 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 dir flaws in Rocket Servergraph Ad Tivoli Storage Manager. The iss fileRequestor servlet, allowing a to write ... **Platforms**: linux, unix, win **CVEs**: CVE-2014-3914 **Refs**: source

Metasploit Module	Date	Rank	Details
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 vulnerability in the Struts Show Struts 1 plugin example in Strut Remote Code Execution can b 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 o Java Web Server prior to versio sending an "OPTIONS" reques long path, attackers can execut In order to ... **Platforms**: linux, solaris, win **CVEs**: CVE-2010-0361 **Refs**: source
JBoss JMX Console Beanshell Deployer WAR Upload and Deployment exploit/multi/http/jboss_bshdeployer	2010-04-26	excellent	This module can be used to ins payload on JBoss servers that "jmx-console" application. The 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 clas Application Server (jbossas) to which then deploys the WAR fil **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 ex on JBoss servers that have an HTTPAdaptor's JMX Invoker ex "JMXInvokerServlet". By invoki 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 ex on JBoss servers that have an console" application. The paylo server by using the jboss.syste functionality. To ... **Platforms**: java, linux, win **CVEs**: CVE-2007-1036, CVE-2 **Refs**: source, ref1, ref2
JBoss Seam 2 File Upload and Execute exploit/multi/http/jboss_seam_upload_exec	2010-08-05	normal	Versions of the JBoss Seam 2 2.2.1CR2 fails to properly sanit some JBoss Expression Langu As a result, attackers can gain execution through the ... **Platforms**: java **CVEs**: CVE-2010-1871 **Refs**: source, ref1, ref2, ref3
Jenkins-CI Script-Console Java Execution exploit/multi/http/jenkins_script_console	2013-01-18	good	This module uses the Jenkins- console to execute OS comma **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 vulnerability in Jenkins versions 1.650 and Jenkins LTS version 1.642.2 which is caused by uns deserialization in XStream with **Platforms**: linux, python, unix, **CVEs**: CVE-2016-0792 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Atlassian HipChat for Jira Plugin Velocity Template Injection exploit/multi/http/jira_hipchat_template	2015-10-28	excellent	Atlassian Hipchat is a web serv instant messaging. A plugin is a that allows team collaboration a message can be used to inject ... **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 ex on Atlassian Jira via the Univer Manager(UPM). The module re credentials to an account that h plugin manager. ... **Platforms**: java **Refs**: source, ref1, ref2, ref3
Kong Gateway Admin API Remote Code Execution exploit/multi/http/kong_gateway_admin_api_rce	2020-10-13	excellent	This module uses the Kong adr a route and a serverless functio associated with the route. The code and is used to run a syste using ... **Platforms**: linux, unix **Refs**: source, ref1, ref2, ref3
ManageEngine Multiple Products Authenticated File Upload exploit/multi/http/manageengine_auth_upload	2014-12-15	excellent	This module exploits a directory vulnerability in ManageEngine AssetExplorer, SupportCenter a uploading attachment files. The 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 uplo ManageEngine ServiceDesk Pl vulnerability exists in the FileUp which accepts unauthenticated 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 inje ManageEngine Security Manag advanced search page, which r code execution under the conte 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 unauth SQL injection in LinkViewFetch exposed in ManageEngine Des build 70200 to v9 build 90033 a 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 arbitra vulnerability in MaraCMS 7.5 a to execute arbitrary commands first attempts to authenticate to then tries to ... **Platforms**: linux, php, win **CVEs**: CVE-2020-25042 **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 vulne when chained allow an attacke unauthenticated remote code e Focus UCMDB. UCMDB includ 2020.05 and below of ... **Platforms**: unix, win **CVEs**: CVE-2020-11853, CVE- **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Th3 MMA mma.php Backdoor Arbitrary File Upload exploit/multi/http/mma_backdoor_upload	2012-04-02	excellent	This module exploits Th3 MMA Backdoor which allows an arbit that leads to arbitrary code exe backdoor also echoes the Linu or operating system ... **Platforms**: php **Refs**: source, ref1
MobileCartly 1.0 Arbitrary File Creation Vulnerability exploit/multi/http/mobilecartly_upload_exec	2012-08-10	excellent	This module exploits a vulnerat MobileCartly. The savepage.ph any permission checks before u file_put_contents(), which allow have direct control of that ... **Platforms**: linux, php **Refs**: source
Moodle Remote Command Execution exploit/multi/http/moodle_cmd_exec	2013-10-30	good	Moodle allows an authenticatec spellcheck settings via the web user can update the spellcheck point to a system-installed aspe updating the ... **Platforms**: linux, unix **CVEs**: CVE-2013-3630 **Refs**: source, ref1
Mutiny Remote Command Execution exploit/multi/http/mutiny_subnetmask_exec	2012-10-22	excellent	This module exploits an authen command injection vulnerability appliance. Versions prior to 4.5 vulnerable. In order to exploit th the mutiny user must ... **Platforms**: linux, unix **CVEs**: CVE-2012-3001 **Refs**: source, ref1
Nostromo Directory Traversal Remote Command Execution exploit/multi/http/nostromo_code_exec	2019-10-20	good	This module exploits a remote execution vulnerability in Nostr This issue is caused by a direc the function `http_verify` in nos allowing an attacker ... **Platforms**: linux, unix **CVEs**: CVE-2019-16278 **Refs**: source, ref1
Novell ServiceDesk Authenticated File Upload exploit/multi/http/novell_servicedesk_rce	2016-03-30	excellent	This module exploits an authen file upload via directory traversa code on the target. It has been versions 6.5 and 7.1.0, in Wind 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 th application of NUUO NVRmini can be done by triggering the w command in the upgrade_hand **Platforms**: linux, unix, win **CVEs**: CVE-2018-14933 **Refs**: source, ref1, ref2
OP5 welcome Remote Command Execution exploit/multi/http/op5_welcome	2012-01-05	excellent	This module exploits an arbitra execution vulnerability in OP5 M Ekelow AB has confirmed that versions 5.3.5, 5.4.0, 5.4.2, 5.5 vulnerable. **Platforms**: linux, unix **CVEs**: CVE-2012-0262 **Refs**: source, ref1
Openfire Admin Console Authentication Bypass exploit/multi/http/openfire_auth_bypass	2008-11-10	excellent	This module exploits an authen vulnerability in the administratic Openfire servers. By using this possible to upload/execute a m plugin ... **Platforms**: java, linux, win **CVEs**: CVE-2008-6508 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
OpenMediaVault Cron Remote Command Execution exploit/multi/http/openmediavault_cmd_exec	2013-10-30	excellent	OpenMediaVault allows an autl to create cron jobs as arbitrary system. An attacker can abuse arbitrary commands as any use the system (including ... **Platforms**: linux, unix **CVEs**: CVE-2013-3632 **Refs**: source, ref1
OpenMRS Java Deserialization RCE exploit/multi/http/openmrs_deserialization	2019-02-04	normal	OpenMRS is an open-source p supplies users with a customiz record system. There exists an deserialization vulnerability in tl `webservices.rest` module use **Platforms**: linux, unix **CVEs**: CVE-2018-19276 **Refs**: source, ref1, ref2, ref3
ManageEngine OpManager and Social IT Arbitrary File Upload exploit/multi/http/opmanager_socialit_file_upload	2014-09-27	excellent	This module exploits a file uplo ManageEngine OpManager an vulnerability exists in the FileC which accepts unauthenticated 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 authen and arbitrary file upload in Orac Testing Suite (OATS), version 1 unknown earlier versions, to up 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 vulnerab Forms and Reports to get remc execution on the host. The sho used to disclose information ab second vulnerability ... **Platforms**: linux, win **CVEs**: CVE-2012-3152, CVE-2 **Refs**: source
OrientDB 2.2.x Remote Code Execution exploit/multi/http/orientdb_exec	2017-07-13	good	This module leverages a privile OrientDB to execute unsandbo commands. All versions from 2 should be vulnerable. **Platforms**: linux, unix, vbs, win **CVEs**: CVE-2017-11467 **Refs**: source, ref1, ref2, ref3
PhpTax pfilez Parameter Exec Remote Code Injection exploit/multi/http/phptax_exec	2012-10-08	excellent	This module exploits a vulnerat PhpTax, an income tax report g generating a PDF, the icondraw drawimage.php does not prope pfilez parameter, ... **Platforms**: linux, unix **Refs**: source
Phpwiki Ploticus Remote Code Execution exploit/multi/http/phpwiki_ploticus_exec	2014-09-11	excellent	The Ploticus module in PhpWik remote attackers to execute art command injection. **Platforms**: linux, php **CVEs**: CVE-2014-5519 **Refs**: source, ref1, ref2
Plone and Zope XMLTools Remote Command Execution exploit/multi/http/plone_popen2	2011-10-04	excellent	Unspecified vulnerability in Zop 2.13.x, as used in Plone 4.0.x t 4.1, and 4.2 through 4.2a2, allo attackers to execute arbitrary c vectors related to the ... **Platforms**: linux, unix **CVEs**: CVE-2011-3587 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
PolarBear CMS PHP File Upload Vulnerability exploit/multi/http/polarcms_upload_exec	2012-01-21	excellent	This module exploits a file uplo found in PolarBear CMS By ab upload.php file, a malicious use file to a temp directory without a which results in ... **Platforms**: linux, php **CVEs**: CVE-2013-0803 **Refs**: source
ProcessMaker Plugin Upload exploit/multi/http/processmaker_plugin_upload	2010-08-25	excellent	This module will generate and u to ProcessMaker resulting in ex code as the web server user. C valid user account with Adminis required to ... **Platforms**: php **Refs**: source, ref1
qdPM v7 Arbitrary PHP File Upload Vulnerability exploit/multi/http/qdpm_upload_exec	2012-06-14	excellent	This module exploits a vulnerab qdPM - a web-based project m software. The user profile's pho can be abused to upload any a the victim server ... **Platforms**: linux, php **Refs**: source
Ruby On Rails DoubleTap Development Mode secret_key_base Vulnerability exploit/multi/http/rails_double_tap	2019-03-13	excellent	This module exploits a vulnerab Rails. In development mode, a would use its name as the secr and can be easily extracted by resource ... **Platforms**: linux **CVEs**: CVE-2019-5420 **Refs**: source, ref1, ref2, ref3, re
Ruby on Rails Dynamic Render File Upload Remote Code Execution exploit/multi/http/rails_dynamic_render_code_exec	2016-10-16	excellent	This module exploits a remote vulnerability in the explicit rend leveraging user parameters. Th been tested across multiple ver Rails. The ... **Platforms**: bsd, linux **CVEs**: CVE-2016-0752 **Refs**: source, ref1, ref2, ref3
Sflog! CMS 1.0 Arbitrary File Upload Vulnerability exploit/multi/http/sflog_upload_exec	2012-07-06	excellent	This module exploits multiple d Sflog 1.0. By default, the CMS admin credential of "admin:sec abused to access administrativ as blogs ... **Platforms**: linux, php **Refs**: source
Snortreport nmap.php/nbtscan.php Remote Command Execution exploit/multi/http/snortreport_exec	2011-09-19	excellent	This module exploits an arbitra execution vulnerability in nmap nbtscan.php scripts. **Platforms**: linux, unix **Refs**: source, ref1
SolarWinds Storage Manager Authentication Bypass exploit/multi/http/solarwinds_store_manager_auth_filter	2014-08-19	excellent	This module exploits an authen vulnerability in Solarwinds Stor The vulnerability exists in the AuthenticationFilter, which allo 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 vulnerab Solr <= 8.3.0 which allows rem execution via a custom Velocity Currently, this module only sup authentication. From ... **Platforms**: java, linux, unix, wi **CVEs**: CVE-2019-17558 **Refs**: source, ref1, ref2, ref3, re

Metasploit Module	Date	Rank	Details
SonicWALL GMS 6 Arbitrary File Upload exploit/multi/http/sonicwall_gms_upload	2012-01-17	excellent	This module exploits a code ex SonicWALL GMS. It exploits tw in order to get its objective. An bypass in the Web Administrati 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 vulneral SonicWALL Scrutinizer. The m parameter in exporters.php allc write arbitrary files to the file sy SQL ... **Platforms**: linux, win **CVEs**: CVE-2014-4977 **Refs**: source, ref1, ref2
Splunk Search Remote Code Execution exploit/multi/http/splunk_mappy_exec	2011-12-12	excellent	This module abuses a commar vulnerability in the web based i Splunk 4.2 to 4.2.4. The vulner the 'mappy' search command v 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 whereby a custom application c through the web based interfac 'script' search command a user commands defined in their ... **Platforms**: linux, osx, unix, win **Refs**: source, ref1, ref2, ref3
Spreecommerce Arbitrary Command Execution exploit/multi/http/spree_searchlogic_exec	2011-04-19	excellent	This module exploits an arbitra execution vulnerability in the Sp API searchlogic for versions 0.5 Unvalidated input is called via t method allowing ... **Platforms**: linux, unix **Refs**: source, ref1
Spreecommerce 0.60.1 Arbitrary Command Execution exploit/multi/http/spree_search_exec	2011-10-05	excellent	This module exploits an arbitra execution vulnerability in the Sp search. Unvalidated input is ca send method allowing comman **Platforms**: linux, unix **Refs**: source, ref1
Apache Struts Jakarta Multipart Parser OGNL Injection exploit/multi/http/struts2_content_type_ognl	2017-03-07	excellent	This module exploits a remote vulnerability in Apache Struts v 2.3.31, and 2.5 - 2.5.10. Remot Execution can be performed via Type header. Native ... **Platforms**: linux, unix, win **CVEs**: CVE-2017-5638 **Refs**: source, ref1
Apache Struts 2 Forced Multi OGNL Evaluation exploit/multi/http/struts2_multi_eval_ognl	2020-09-14	excellent	The Apache Struts framework, performs double evaluation of a assigned to certain tags attribut is therefore possible to pass in that ... **Platforms**: linux, unix **CVEs**: CVE-2019-0230, CVE-2 **Refs**: source, ref1, ref2, ref3, re
Apache Struts 2 Namespace Redirect OGNL Injection exploit/multi/http/struts2_namespace_ognl	2018-08-22	excellent	This module exploits a remote vulnerability in Apache Struts v 2.3.4, and 2.5 - 2.5.16. Remote can be performed via an endpo use of a redirect ... **Platforms**: linux, unix, win **CVEs**: CVE-2018-11776 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Apache Struts 2 REST Plugin XStream RCE exploit/multi/http/struts2_rest_xstream	2017-09-05	excellent	Apache Struts versions 2.1.2 - 2.5 - Struts 2.5.12, using the RI vulnerable to a Java deserializa XStream library. **Platforms**: linux, python, unix, **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 execution vulnerability in Apach versions < 2.2.0. This issue is c failure to properly handle unico 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 execution vulnerability in Apach versions 1.x (<= 1.3.10) and 2.: Struts 1.x the problem is relate ActionForm bean population ... **Platforms**: linux, win **CVEs**: CVE-2014-0094, CVE-2 2014-0114 **Refs**: source, ref1, ref2, ref3, re
Apache Struts Remote Command Execution exploit/multi/http/struts_code_exec_exception_delegator	2012-01-06	excellent	This module exploits a remote execution vulnerability in Apach versions < 2.2.1.1. This issue is because the ExceptionDelegat parameter values as OGNL exp **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 execution vulnerability in Apach versions < 2.3.1.2. This issue is because the ParametersInterce the use of parentheses which ir **Platforms**: java, linux, win **CVEs**: CVE-2011-3923 **Refs**: source, ref1, ref2
Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution exploit/multi/http/struts_default_action_mapper	2013-07-02	excellent	The Struts 2 DefaultActionMap method for short-circuit navigat changes by prefixing paramete or "redirect: followed by a desir 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 execution vulnerability in Apach between 2.3.20 and 2.3.28 (exc 2.3.24.2). Remote Code Execu 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 execution vulnerability in Apach between 2.3.20 and 2.3.28 (exc 2.3.24.2). Remote Code Execu 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 execution vulnerability in Apach versions < 2.3.14.2. A specifica request parameter can be usec arbitrary OGNL code into the st **Platforms**: java, linux, win **CVEs**: CVE-2013-1966, CVE-2 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
SysAid Help Desk Administrator Portal Arbitrary File Upload exploit/multi/http/sysaid_auth_file_upload	2015-06-03	excellent	This module exploits a file uplo SysAid Help Desk. The vulnera ChangePhoto.jsp in the admini which does not correctly handle 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 uplo SysAid Help Desk v14.3 and v1 vulnerability exists in the RdsLo which accepts unauthenticated 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 payl 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 ex on Apache Tomcat servers that exposed "manager" application uploaded as a WAR archive co application using a PUT ... **Platforms**: java, linux, win **CVEs**: CVE-2009-3548, CVE-2 2009-4188, CVE-2009-4189, C CVE-2010-4094 **Refs**: source, ref1, ref2
Apache Tomcat Manager Authenticated Upload Code Execution exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	This module can be used to ex on Apache Tomcat servers that exposed "manager" application uploaded as a WAR archive co application using a POST ... **Platforms**: java, linux, win **CVEs**: CVE-2009-3548, CVE-2 2009-4188, CVE-2009-4189, C CVE-2010-4094 **Refs**: source, ref1, ref2
Total.js CMS 12 Widget JavaScript Code Injection exploit/multi/http/totaljs_cms_widget_exec	2019-08-30	excellent	This module exploits a vulnerab CMS. The issue is that a user v permission can embed a malici payload in a widget, which is ev side, and gain ... **Platforms**: linux, osx, wget **CVEs**: CVE-2019-15954 **Refs**: source, ref1, ref2
Trend Micro Threat Discovery Appliance admin_sys_time.cgi Remote Command Execution exploit/multi/http/trendmicro_threat_discovery_admin_sys_time_cmdi	2017-04-10	excellent	This module exploits two vulne Trend Micro Threat Discovery A first is an authentication bypass a file delete in logoff.cgi which r ... **Platforms**: linux **CVEs**: CVE-2016-7547, CVE-2 **Refs**: source, ref1
vBulletin /ajax/api/content_infraction/getIndexableContent nodeid Parameter SQL Injection exploit/multi/http/vbulletin_getindexablecontent	2020-03-12	manual	This module exploits a SQL inje vulnerability found in vBulletin 5 This module uses the getIndex vulnerability to reset the admini password, it then uses the ... **Platforms**: php **CVEs**: CVE-2020-12720 **Refs**: source
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 bu template rendering code in vBu module uses the vBulletin temp functionality to render the 'widget_tabbedcontainer_tab_p **Platforms**: php, unix, win **CVEs**: CVE-2019-16759, CVE- **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Visual Mining NetCharts Server Remote Code Execution exploit/multi/http/visual_mining_netcharts_upload	2014-11-03	excellent	This module exploits multiple v Visual Mining NetCharts. First, validation in the administration arbitrary jsp code upload to loc ... **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 unauth file upload and path traversal ir vCenter Server to write a JSP p accessible directory. Fixed vers Update 3n, 6.7 Update ... **Platforms**: linux, win **CVEs**: CVE-2021-21972 **Refs**: source, ref1, ref2, ref3, re ref7
Oracle WebLogic Server Administration Console Handle RCE exploit/multi/http/weblogic_admin_handle_rce	2020-10-20	excellent	This module exploits a path tra Java class instantiation in the h implementation of WebLogic's A Console to execute code as the Versions 10.3.6.0.0, ... **Platforms**: linux, unix, win **CVEs**: CVE-2020-14750, CVE- 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 vulnerab Framework Server 5.2 that allo unauthenticated user to upload using a directory traversal attac FileUploadServlet servlet. A ... **Platforms**: linux, win **CVEs**: CVE-2016-6600 **Refs**: source, ref1, ref2
WP Database Backup RCE exploit/multi/http/wp_db_backup_rce	2019-04-24	excellent	There exists a command injecti in the Wordpress plugin `wp-da for versions < 5.2. For the back the plugin generates a `mysqld to execute. ... **Platforms**: linux, win **Refs**: source, ref1
Zabbix Authenticated Remote Command Execution exploit/multi/http/zabbix_script_exec	2013-10-30	excellent	ZABBIX allows an administrato that will be run on hosts. An au attacker can create a script cor payload, then a host with an IP run the ... **Platforms**: linux, unix **CVEs**: CVE-2013-3628 **Refs**: source, ref1
Novell ZENworks Configuration Management Arbitrary File Upload exploit/multi/http/zenworks_configuration_management_upload	2015-04-07	excellent	This module exploits a file uplo Novell ZENworks Configuratior (ZCM, which is part of the ZEN The vulnerability exists in the U 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 ex Novell ZENworks Configuratior SP3 and 11 SP2. The vulnerab ZENworks Control Center appli an ... **Platforms**: linux, win **CVEs**: CVE-2013-1080 **Refs**: source, ref1
Zpanel Remote Unauthenticated RCE exploit/multi/http/zpanel_information_disclosure_rce	2014-01-30	excellent	This module exploits an informa vulnerability in ZPanel. The vul to a vulnerable version of pCha ZPanel that allows unauthentic read arbitrary ... **Platforms**: linux, php **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Snort 2 DCE/RPC Preprocessor Buffer Overflow exploit/multi/ids/snort_dce_rpc	2007-02-19	good	This module allows remote atta arbitrary code by exploiting the crafted SMB traffic. The vulnera boundary error within the DCE/ preprocessor ... **Platforms**: linux, win **CVEs**: CVE-2006-5276 **Refs**: source, ref1, ref2, ref3
MagniComp SysInfo mcsiwrapper Privilege Escalation exploit/multi/local/magnicomp_sysinfo_mcsiwrapper_priv_esc	2016-09-23	excellent	This module attempts to gain ro systems running MagniComp S prior to 10-H64. The .mcsiwrap executable allows loading a co '--configfile' ... **Platforms**: linux, solaris **CVEs**: CVE-2017-6516 **Refs**: source, ref1, ref2, ref3
Xorg X11 Server SUID logfile Privilege Escalation exploit/multi/local/xorg_x11_suid_server	2018-10-25	good	This module attempts to gain ro SUID Xorg X11 server versions A permission check flaw exists and -logfile options when startir allows ... **Platforms**: linux, openbsd, unix **CVEs**: CVE-2018-14665 **Refs**: source, ref1, ref2
Xorg X11 Server SUID modulepath Privilege Escalation exploit/multi/local/xorg_x11_suid_server_modulepath	2018-10-25	good	This module attempts to gain ro SUID Xorg X11 server versions A permission check flaw exists and -logfile options when startir allows ... **Platforms**: linux, solaris, unix **CVEs**: CVE-2018-14665 **Refs**: source, ref1
Java RMI Server Insecure Default Configuration Java Code Execution exploit/multi/misc/java_rmi_server	2011-10-15	excellent	This module takes advantage o configuration of the RMI Regist Activation services, which allow from any remote (HTTP) URL. method in the RMI ... **Platforms**: java, linux, osx, sola **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 ex Western Digital Arkeia version below. The vulnerability exists i daemon listening on TCP port 6 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 s execute Java Code in the Squig included in the Batik framework crafted SVG file referencing a j 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 rem execution feature provided by t Agent software. It can also be u privileges on Windows hosts as runs as SYSTEM but ... **Platforms**: linux, unix, win **CVEs**: CVE-2018-20735 **Refs**: source, ref1
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 ac check in the BMC Server Autor agent that allows arbitrary oper commands to be executed with authentication. Note: Under Wi **Platforms**: linux, unix, win **CVEs**: CVE-2016-1542, CVE-2 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Nanopool Claymore Dual Miner APIs RCE exploit/multi/misc/claymore_dual_miner_remote_manager_rce	2018-02-09	excellent	This module takes advantage c manager APIs to exploit an RC **Platforms**: linux, win **CVEs**: CVE-2018-1000049 **Refs**: source, ref1
Hashicorp Consul Remote Command Execution via Rexec exploit/multi/misc/consul_rexec_exec	2018-08-11	excellent	This module exploits a feature Consul named rexec. **Platforms**: linux **Refs**: source, ref1, ref2, ref3
Hashicorp Consul Remote Command Execution via Services API exploit/multi/misc/consul_service_exec	2018-08-11	excellent	This module exploits Hashicorp services API to gain remote co 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 daemo coordinate distributed erlang in an attacker get the authenticati trivial. Usually, this cookie is na ".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 FreeSWI socket interface to execute sys using the `system` API comma socket service is enabled by de 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 vulnerabi Data Protector. The vulnerabilit Backup client service, which lis on TCP/5555. The EXEC_INTE allows to execute ... **Platforms**: unix, win **Refs**: source
HP StorageWorks P4000 Virtual SAN Appliance Command Execution exploit/multi/misc/hp_vsa_exec	2011-11-11	excellent	This module exploits a vulnerat HP's StorageWorks P4000 VSA prior to 9.5. By using a default credential, it is possible to injec commands as part of a ... **Platforms**: linux, unix **CVEs**: CVE-2012-4361 **Refs**: source, ref1, ref2, ref3
IBM TM1 / Planning Analytics Unauthenticated Remote Code Execution exploit/multi/misc/ibm_tm1_unauth_rce	2019-12-19	excellent	This module exploits a vulnerat / Planning Analytics that allows unauthenticated attacker to per configuration overwrite. It starts Admin server for the ... **Platforms**: linux, unix, win **CVEs**: CVE-2019-4716 **Refs**: source, ref1, ref2, ref3
Java Debug Wire Protocol Remote Code Execution exploit/multi/misc/java_jdwp_debugger	2010-03-12	good	This module abuses exposed J Protocol services in order to ex Java code remotely. It just abus features, since no authenticatic the service ... **Platforms**: linux, osx, win **Refs**: source, ref1, ref2, ref3, re
Eclipse Equinoxe OSGi Console Command Execution exploit/multi/misc/osgi_console_exec	2018-02-13	normal	Exploit Eclipse Equinoxe OSGi Gateway initiative) console 'forl execute arbitrary commands or system. **Platforms**: linux, win **Refs**: source, ref1
TeamCity Agent XML-RPC Command Execution exploit/multi/misc/teamcity_agent_xmlrpc_exec	2015-04-14	excellent	This module allows remote cod TeamCity Agents configured to communication via xml-rpc. In t mode the TeamCity server pusl commands to the Build ... **Platforms**: linux, win **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
VERITAS NetBackup Remote Command Execution exploit/multi/misc/veritas_netbackup_cmdexec	2004-10-21	excellent	This module allows arbitrary co execution on an ephemeral por Veritas NetBackup, whilst an ac authenticated. The port is open direct console access as root .. **Platforms**: linux, unix, win **CVEs**: CVE-2004-1389 **Refs**: source
WebLogic Server Deserialization RCE - BadAttributeValueExpException exploit/multi/misc/weblogic_deserialize_badattrval	2020-01-15	normal	There exists a Java object dese vulnerability in multiple versions Unauthenticated remote code e achieved by sending a serialize BadAttributeValueExpExceptio **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 dese vulnerability in multiple versions Unauthenticated remote code e achieved by sending a serialize **Platforms**: linux, unix, win **CVEs**: CVE-2020-2883 **Refs**: source, ref1
Wireshark LWRES Dissector getaddrsbyname_request Buffer Overflow exploit/multi/misc/wireshark_lwres_getaddrbyname	2010-01-27	great	The LWRES dissector in Wires 0.9.15 through 1.0.10 and 1.2.0 allows remote attackers to exec code due to a stack-based buff 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 Wires 0.9.15 through 1.0.10 and 1.2.0 allows remote attackers to exec code due to a stack-based buff bug found and ... **Platforms**: linux, osx, win **CVEs**: CVE-2010-0304 **Refs**: source, ref1, ref2
Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution exploit/multi/misc/xdh_x_exec	2015-12-04	excellent	This module allows remote con on an IRC Bot developed by xd was caught by Conor Patrick w honeypot server and is categor Zanke as an fBot ... **Platforms**: unix, win **Refs**: source, ref1, ref2, ref3
Oracle MySQL UDF Payload Execution exploit/multi/mysql/mysql_udf_payload	2009-01-16	excellent	This module creates and enabl (user defined function) on the ta SELECT . into DUMPFILE met injection. On default Microsoft V installations of MySQL ... **Platforms**: linux, win **Refs**: source, ref1
NTP Daemon readvar Buffer Overflow exploit/multi/ntp/ntp_overflow	2001-04-04	good	This module exploits a stack ba overflow in the ntpd and xntpd sending an overly long 'readvar possible to execute code remot is corrupted, this ... **Platforms**: linux **CVEs**: CVE-2001-0414 **Refs**: source
PHP 4 unserialize() ZVAL Reference Counter Overflow (Cookie) exploit/multi/php/php_unserialize_zval_cookie	2007-03-04	average	This module exploits an integer vulnerability in the unserialize() PHP web server extension. Thi was patched by Stefan in versi applies all ... **Platforms**: linux **CVEs**: CVE-2007-1286 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
PostgreSQL COPY FROM PROGRAM Command Execution exploit/multi/postgres/postgres_copy_from_program_cmd_exec	2019-03-20	excellent	Installations running Postgres 9 have functionality which allows superuser and users with 'pg_execute_server_program' t from an external program using **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 configured to allow loading exte languages. Most commonly this Python. When enabled, comma 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 o RealServer 7/8/9 and was base Cyberpunk's THCrealbad explo should reliably exploit Linux, BS Windows-based servers. **Platforms**: bsd, linux, win **CVEs**: CVE-2002-1643 **Refs**: source
Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow exploit/multi/samba/nttrans	2003-04-07	average	This module attempts to exploit overflow vulnerability present ir through 2.2.6 of Samba. The S report this as: "Bug in the lengt encrypted ... **Platforms**: linux **CVEs**: CVE-2002-1318 **Refs**: source, ref1
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-2 vulnerability within the SAP EE (tc~smd~agent~application~ee Solution Manager (SolMan) rur 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 arbitr through the SAP Management Interface. A valid username an the SAP Management Console provided. This module has bee **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 N SXPG_CALL_SYSTEM functio SOAP RFC Service, to execute commands. This module needs with privileges to use the /sap/b **Platforms**: unix, win **Refs**: source, ref1
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 N SXPG_COMMAND_EXECUTE SAP SOAP RFC Service, to ex commands. This module needs 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 de vulnerability in the Inductive Au SCADA product, versions 8.0.0 including) 8.0.7. This exploit wa versions 8.0.0 and ... **Platforms**: unix, win **CVEs**: CVE-2020-10644, CVE- **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Rank	Details
Script Web Delivery exploit/multi/script/web_delivery	2013-07-19	manual	This module quickly fires up a v serves a payload. The module command to be run on the targ based on the selected target. T command will download and ... **Platforms**: linux, osx, php, pyth **Refs**: source, ref1, ref2, ref3, re ref7, ref8, ref9, ref10
SSH User Code Execution exploit/multi/ssh/sshexec	1999-01-01	manual	This module connects to the ta executes the necessary comma specified payload via SSH. If a specified, an appropriate stage **Platforms**: bsd, linux, osx, pyth **CVEs**: CVE-1999-0502 **Refs**: source
Subversion Date Svnserve exploit/multi/svn/svnserve_date	2004-05-19	average	This is an exploit for the Subve parsing overflow. This exploit is daemon (svn:// protocol) and w Subversion over webdav (http[s should ... **Platforms**: bsd, linux **CVEs**: CVE-2004-0397 **Refs**: source, ref1
VNC Keyboard Remote Code Execution exploit/multi/vnc/vnc_keyboard_exec	2015-07-10	great	This module exploits VNC serv virtual keyboard keys and exec On Windows systems a comma opened and a PowerShell or C 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 bu Tinc's tincd service. After authe specially crafted tcp packet (de leads to a buffer overflow and a ... **Platforms**: bsd, linux, offset, ur **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 service by pretending to be a le This process involves starting b FTP services on the attacker si contacting the ... **Platforms**: linux, win **CVEs**: CVE-2009-0695 **Refs**: source, ref1, ref2
DHCP Client Command Injection (DynoRoot) exploit/unix/dhcp/rhel_dhcp_client_command_injection	2018-05-15	excellent	This module exploits the DynoR a flaw in how the NetworkMana script included in the DHCP clie Enterprise Linux 6 and 7, Fedo processes ... **Platforms**: unix **CVEs**: CVE-2018-1111 **Refs**: source, ref1, ref2, ref3, re ref7
Pi-Hole Whitelist OS Command Execution exploit/unix/http/pihole_whitelist_exec	2018-04-15	excellent	This exploits a command execu in Pi-Hole <= 3.3. When adding to the whitelist, it is possible to command to the domain that is **Platforms**: linux **Refs**: source, ref1
VMTurbo Operations Manager vmtadmin.cgi Remote Command Execution exploit/unix/http/vmturbo_vmtadmin_exec_noauth	2014-06-25	excellent	VMTurbo Operations Manager vulnerable to unauthenticated C injection in the web interface. U payloads for the most reliable r a blind OS ... **Platforms**: linux, unix **CVEs**: CVE-2014-5073 **Refs**: source, ref1

Metasploit Module	Date	Rank	Details
Setuid Nmap Exploit exploit/unix/local/setuid_nmap	2012-07-19	excellent	Nmap's man page mentions tha never be installed with special suid root) for security reasons." avoids making any of its binarie ... **Platforms**: bsd, linux, unix **Refs**: source
Arista restricted shell escape (with privesc) exploit/unix/ssh/arista_tacplus_shell	2020-02-02	great	This exploit module takes adva configured TACACS+ config, A and TACACS+ read-only accou escalate. A CVSS v3 base scor been assigned. **Platforms**: linux **CVEs**: CVE-2020-9015 **Refs**: source, ref1, ref2, ref3
Basilic 1.5.14 diff.php Arbitrary Command Execution exploit/unix/webapp/basilic_diff_exec	2012-06-28	excellent	This module abuses a metacha vulnerability in the diff.php scrip allows an unauthenticated attac arbitrary commands as the ww account. **Platforms**: linux, unix **CVEs**: CVE-2012-3399 **Refs**: source
Bolt CMS 3.7.0 - Authenticated Remote Code Execution exploit/unix/webapp/bolt_authenticated_rce	2020-05-07	excellent	This module exploits multiple v Bolt CMS version 3.7.0 and 3.6 execute arbitrary commands as running Bolt. This module first t of a vulnerability ... **Platforms**: linux, unix **Refs**: source, ref1
Dogfood CRM spell.php Remote Command Execution exploit/unix/webapp/dogfood_spell_exec	2009-03-03	excellent	This module exploits a previous vulnerability in the Dogfood CR which is vulnerable to comman spell check feature. Because o restrictions, ... **Platforms**: linux, unix, win **Refs**: source, ref1
Drupal Drupalgeddon 2 Forms API Property Injection exploit/unix/webapp/drupal_drupalgeddon2	2018-03-28	excellent	This module exploits a Drupal in the Forms API. Drupal 6.x, < 8.3.9, < 8.4.6, and < 8.5.1 are **Platforms**: linux, php, unix **CVEs**: CVE-2018-7600 **Refs**: source, ref1, ref2, ref3, re
FusionPBX Command exec.php Command Execution exploit/unix/webapp/fusionpbx_exec_cmd_exec	2019-11-02	excellent	This module uses administrativ available in FusionPBX to gain Command section of the applic users with `exec_view` permiss superadmin permissions, to ... **Platforms**: linux, php, unix **Refs**: source, ref1
FusionPBX Operator Panel exec.php Command Execution exploit/unix/webapp/fusionpbx_operator_panel_exec_cmd_exec	2019-06-06	excellent	This module exploits an authen command injection vulnerability versions 4.4.3 and prior. The `e within the Operator Panel perm `operator_panel_view` ... **Platforms**: linux, unix **CVEs**: CVE-2019-11409 **Refs**: source, ref1, ref2
Matt Wright guestbook.pl Arbitrary Command Execution exploit/unix/webapp/guestbook_ssi_exec	1999-11-05	excellent	The Matt Wright guestbook.pl < script contains a flaw that may command execution. The vulne that HTML posting is enabled i guestbook.pl script, and ... **Platforms**: linux, unix, win **CVEs**: CVE-1999-1053 **Refs**: source
Havalite CMS Arbitary File Upload Vulnerability exploit/unix/webapp/havalite_upload_exec	2013-06-17	excellent	This module exploits a file uplo found in Havalite CMS 1.1.7, a Attackers can abuse the upload to upload a malicious PHP file **Platforms**: linux, php **Refs**: source

Metasploit Module	Date	Rank	Details
blueimp's jQuery (Arbitrary) File Upload exploit/unix/webapp/jquery_file_upload	2018-10-09	excellent	This module exploits an arbitra the sample PHP upload handle jQuery File Upload widget in ve Due to a default configuration i the ... **Platforms**: linux, php **CVEs**: CVE-2018-9206 **Refs**: source, ref1, ref2, ref3, re
LibrettoCMS File Manager Arbitary File Upload Vulnerability exploit/unix/webapp/libretto_upload_exec	2013-06-14	excellent	This module exploits a file uplo found in LibrettoCMS 1.1.7, an Attackers can bypass the file e and abuse the upload feature i a ... **Platforms**: linux, php **Refs**: source
Mitel Audio and Web Conferencing Command Injection exploit/unix/webapp/mitel_awc_exec	2010-12-12	excellent	This module exploits a comma within the Mitel Audio and Web web interface. **Platforms**: linux, unix **Refs**: source
Nagios3 history.cgi Host Command Execution exploit/unix/webapp/nagios3_history_cgi	2012-12-09	great	This module abuses a comma vulnerability in the Nagios3 hist **Platforms**: linux, unix **CVEs**: CVE-2012-6096 **Refs**: source
Narcissus Image Configuration Passthru Vulnerability exploit/unix/webapp/narcissus_backend_exec	2012-11-14	excellent	This module exploits a vulnerab Narcissus image configuration due to the backend.php file not $release parameter properly, a on to the ... **Platforms**: linux, unix **Refs**: source
OpenMediaVault rpc.php Authenticated PHP Code Injection exploit/unix/webapp/openmediavault_rpc_rce	2020-09-28	excellent	This module exploits an authen code injection vulnerability four openmediavault versions befor versions before 5.5.12 inclusive POST parameter of the ... **Platforms**: linux, unix **CVEs**: CVE-2020-26124 **Refs**: source, ref1
OpenNetAdmin Ping Command Injection exploit/unix/webapp/opennetadmin_ping_cmd_injection	2019-11-19	excellent	This module exploits a comma OpenNetAdmin between 8.5.14 **Platforms**: linux **Refs**: source
Oracle VM Server Virtual Server Agent Command Injection exploit/unix/webapp/oracle_vm_agent_utl	2010-10-12	excellent	This module exploits a comma within Oracle's VM Server Virtu (ovs-agent) service. By includir characters within the second pa 'utl_test_url' ... **Platforms**: linux, unix **CVEs**: CVE-2010-3585 **Refs**: source
Project Pier Arbitrary File Upload Vulnerability exploit/unix/webapp/projectpier_upload_exec	2012-10-08	excellent	This module exploits a vulnerab Project Pier. The application's u does not require any authentica allows a malicious user to uploa file onto the ... **Platforms**: linux, php **Refs**: source
rConfig install Command Execution exploit/unix/webapp/rconfig_install_cmd_exec	2019-10-28	excellent	This module exploits an unauth command injection vulnerability versions 3.9.2 and prior. The `in not automatically removed afte allowing ... **Platforms**: linux, unix **CVEs**: CVE-2019-16662, CVE- **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
SPIP connect Parameter PHP Injection exploit/unix/webapp/spip_connect_exec	2012-07-04	excellent	This module exploits a PHP co SPIP. The vulnerability exists ir parameter and allows an unaut to execute arbitrary commands privileges. ... **Platforms**: php **Refs**: source, ref1
ThinkPHP Multiple PHP Injection RCEs exploit/unix/webapp/thinkphp_rce	2018-12-10	excellent	This module exploits one of two vulnerabilities in the ThinkPHP to execute code as the web use and including 5.0.23 are exploit 5.0.23 is ... **Platforms**: linux, unix **CVEs**: CVE-2018-20062, CVE- **Refs**: source, ref1, ref2
TrixBox CE endpoint_devicemap.php Authenticated Command Execution exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce	2020-04-28	excellent	This module exploits an authen command injection vulnerability CE version 1.2.0 to 2.8.0.4 incl "network" POST parameter of t **Platforms**: linux, unix **CVEs**: CVE-2020-7351 **Refs**: source, ref1
vBulletin index.php/ajax/api/reputation/vote nodeid Parameter SQL Injection exploit/unix/webapp/vbulletin_vote_sqli_exec	2013-03-25	excellent	This module exploits a SQL inje vulnerability found in vBulletin 5 used in the wild since March 20 uses the sqli to extract the web usernames and ... **Platforms**: php **CVEs**: CVE-2013-3522 **Refs**: source, ref1
WordPress PHPMailer Host Header Command Injection exploit/unix/webapp/wp_phpmailer_host_header	2017-05-03	average	This module exploits a comma vulnerability in WordPress vers as an MTA via a spoofed Host PHPMailer, a mail-sending libra bundled with WordPress. A ... **Platforms**: linux **CVEs**: CVE-2016-10033 **Refs**: source, ref1, ref2, ref3
Xymon useradm Command Execution exploit/unix/webapp/xymon_useradm_cmd_exec	2016-02-14	excellent	This module exploits a comma vulnerability in Xymon versions which allows authenticated use arbitrary operating system com web server user. When ... **Platforms**: bsd, linux, solaris, u **CVEs**: CVE-2016-2056 **Refs**: source, ref1, ref2, ref3, re
ZeroShell Remote Code Execution exploit/unix/webapp/zeroshell_exec	2013-09-22	excellent	This module exploits a vulnerab ZeroShell 2.0 RC2 and lower. I unauthenticated local file inclus in the "/cgi-bin/kerbynet" url. Th ... **Platforms**: linux **CVEs**: CVE-2009-0545 **Refs**: source
Zimbra Collaboration Server LFI exploit/unix/webapp/zimbra_lfi	2013-12-06	excellent	This module exploits a local file Zimbra 8.0.2 and 7.2.2. The vu an attacker to get the LDAP cre localconfig.xml file. The stolen the ... **Platforms**: linux **CVEs**: CVE-2013-7091 **Refs**: source, ref1
Novell ZENworks Configuration Management Remote Execution exploit/windows/http/zenworks_uploadservlet	2010-03-30	excellent	This module exploits a code ex Novell ZENworks Configuration 10.2.0. By exploiting the Uploa attacker can upload a malicious the TEMP directory ... **Platforms**: java, linux, win **CVEs**: CVE-2010-5324 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
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 authen file upload and code execution Backup v7.x - v8.1.1.50. To suc the upload credentials are neec Ahsay Backup ... **Platforms**: linux, win **CVEs**: CVE-2019-10267 **Refs**: source, ref1, ref2

Showing 1 to 573 of 573 entries

How to search for exploits in Metasploit

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

List all exploits:

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

Find exploit by CVE:

```
msf6 > search type:exploit cve:2020
```

Search exploits by port:

```
msf6 > search type:exploit port:22
```

Find exploit by name:

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

Search exploits by OS (platform):

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

Search exploits by OS (target):

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

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 Linux 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 Windows Exploits (Detailed Spreadsheet)
- Metasploit Auxiliary Modules (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 | Exploitation | Linux | Metasploit | Msfconsole | Privilege escalation | RCE | Spreadsheet