Cisco » Unified Computing System : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **53** Page : 1 (This Page) 2

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-44228	20		Exec Code	2021-12-10	2023-04-03	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

2	CVE-2020-10136	290		Bypass	2020-06-02	2020-07-29	5.0	None	Remote	Low	Not required	None	None	Partial

Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors.

3	CVE-2019-1966			Exec Code +Priv	2019-08-30	2020-10-16	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in a specific CLI command within the local management (local-mgmt) context for Cisco UCS Fabric Interconnect Software could allow an authenticated, local attacker to gain elevated privileges as the root user on an affected device. The vulnerability is due to extraneous subcommand options present for a specific CLI command within the local-mgmt context. An attacker could exploit this vulnerability by authenticating to an affected device, entering the local-mgmt context, and issuing a specific CLI command and submitting user input. A successful exploit could allow the attacker to execute arbitrary operating system commands as root on an affected device. The attacker would need to have valid user credentials for the device.

4	CVE-2019-1908				2019-08-21	2020-10-16	5.0	None	Remote	Low	Not required	Partial	None	None

A vulnerability in the Intelligent Platform Management Interface (IPMI) implementation of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to view sensitive system information. The vulnerability is due to insufficient security restrictions imposed by the affected software. A successful exploit could allow the attacker to view sensitive information that belongs to other users. The attacker could then use this information to conduct additional attacks.

5	CVE-2019-1907			+Priv	2019-08-21	2020-10-16	6.5	None	Remote	Low	???	Partial	Partial	Partial

A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to set sensitive configuration values and gain elevated privileges. The vulnerability is due to improper handling of substring comparison operations that are performed by the affected software. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow the attacker with read-only privileges to gain administrator privileges.

6	CVE-2019-1900	476		DoS	2019-08-21	2023-03-31	7.8	None	Remote	Low	Not required	None	None	Complete

A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to cause the web server process to crash, causing a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient validation of user-supplied input on the web interface. An attacker could exploit this vulnerability by submitting a crafted HTTP request to certain endpoints of the affected software. A successful exploit could allow an attacker to cause the web server to crash. Physical access to the device may be required for a restart.

7	CVE-2019-1896	78		Exec Code	2019-08-21	2023-03-31	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to inject arbitrary commands and obtain root privileges. The vulnerability is due to insufficient validation of user-supplied input in the Certificate Signing Request (CSR) function of the web-based management interface. An attacker could exploit this vulnerability by submitting a crafted CSR in the web-based management interface. A successful exploit could allow an attacker with administrator privileges to execute arbitrary commands on the device with full root privileges.

8	CVE-2019-1885	78		Exec Code	2019-08-21	2023-03-31	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the Redfish protocol of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to inject and execute arbitrary commands with root privileges on an affected device. The vulnerability is due to insufficient validation of user-supplied input by the affected software. An attacker could exploit this vulnerability by sending crafted authenticated commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to inject and execute arbitrary commands on an affected device with root privileges.

9	CVE-2019-1883	78		Exec Code	2019-08-21	2023-03-31	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in the command-line interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker with read-only credentials to inject arbitrary commands that could allow them to obtain root privileges. The vulnerability is due to insufficient validation of user-supplied input on the command-line interface. An attacker could exploit this vulnerability by authenticating with read-only privileges via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow an attacker to execute arbitrary commands on

the device with root privileges.

10	CVE-2019-1879	78	Exec Code	2019-06-20	2019-10-09	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in the CLI of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient validation of user-supplied input at the CLI. An attacker could exploit this vulnerability by authenticating with the administrator password via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute arbitrary commands on the device with root privileges.

11	CVE-2019-1871	119	DoS Overflow	2019-08-21	2019-10-09	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the Import Cisco IMC configuration utility of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition and implement arbitrary commands with root privileges on an affected device. The vulnerability is due to improper bounds checking by the import-config process. An attacker could exploit this vulnerability by sending malicious packets to an affected device. When the packets are processed, an exploitable buffer overflow condition may occur. A successful exploit could allow the attacker to implement arbitrary code on the affected device with elevated privileges.

12	CVE-2019-1865	78	Exec Code	2019-08-21	2023-03-31	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges on an affected device. The vulnerability is due to insufficient validation of user-supplied input by the affected software. An attacker could exploit this vulnerability by invoking an interface monitoring mechanism with a crafted argument on the affected software. A successful exploit could allow the attacker to inject and execute arbitrary, system-level commands with root privileges on an affected device.

13	CVE-2019-1864	78	Exec Code	2019-08-21	2023-03-31	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges on an affected device. The vulnerability is due to insufficient validation of command input by the affected software. An attacker could exploit this vulnerability by sending malicious commands to the web-based management interface of the affected software. A successful exploit could allow the attacker, with read-only privileges, to inject and execute arbitrary, system-level commands with root privileges on an affected device.

14	CVE-2019-1863			2019-08-21	2020-10-16	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to make unauthorized changes to the system configuration. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow a user with read-only privileges to change critical system configurations using administrator privileges.

15	CVE-2019-1850	78	Exec Code	2019-08-21	2019-10-09	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges on an affected device. An attacker would need to have valid administrator credentials on the device. The vulnerability is due to insufficient validation of user-supplied input by the affected software. An attacker with elevated privileges could exploit this vulnerability by sending crafted commands to the administrative web management interface of the affected software. A successful exploit could allow the attacker to inject and execute arbitrary, system-level commands with root privileges on an affected device.

16	CVE-2019-1736	347	Bypass	2020-09-23	2020-10-23	6.9	None	Local	Medium	Not required	Complete	Complete	Complete

A vulnerability in the firmware of the Cisco UCS C-Series Rack Servers could allow an authenticated, physical attacker to bypass Unified Extensible Firmware Interface (UEFI) Secure Boot validation checks and load a compromised software image on an affected device. The vulnerability is due to improper validation of the server firmware upgrade images. An attacker could exploit this vulnerability by installing a server firmware version that would allow the attacker to disable UEFI Secure Boot. A successful exploit could allow the attacker to bypass the signature validation checks that are done by UEFI Secure Boot technology and load a compromised software image on the affected device. A compromised software image is any software image that has not been digitally signed by Cisco.

17	CVE-2019-1725	78		2019-04-18	2020-10-08	3.6	None	Local	Low	Not required	None	Partial	Partial

A vulnerability in the local management CLI implementation for specific commands on the Cisco UCS B-Series Blade Servers could allow an authenticated, local attacker to overwrite an arbitrary file on disk. It is also possible the attacker could inject CLI command parameters that should not be allowed for a specific subset of local management CLI commands. The vulnerability is due to lack of proper input validation of user input for local management CLI commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a crafted form of a limited subset of local management CLI commands. An exploit could allow the attacker to overwrite an arbitrary files on disk or inject CLI command parameters that should have been disabled. This vulnerability is fixed in software version 4.0(2a) and later.

18	CVE-2019-1634	78	Exec Code +Priv	2019-08-21	2020-10-16	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the Intelligent Platform Management Interface (IPMI) of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges on the underlying operating system (OS). The vulnerability is due to insufficient input validation of user-supplied commands. An attacker who has administrator privileges and access to the network where the IPMI resides could exploit this vulnerability by submitting crafted input to the affected commands. A successful exploit could allow the attacker to gain root privileges on the affected device.

19	CVE-2019-1632	352	CSRF	2019-06-20	2019-10-09	6.0	None	Remote	Medium	???	Partial	Partial	Partial

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on the

affected device.

20	CVE-2019-1631	306		2019-06-20	2019-10-09	5.0	None	Remote	Low	Not required	Partial	None	None

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to access potentially sensitive system usage information. The vulnerability is due to a lack of proper data protection mechanisms. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow an attacker to view sensitive system data.

21	CVE-2019-1630	119	DoS Overflow Bypass	2019-06-20	2019-10-09	2.1	None	Local	Low	Not required	None	None	Partial

A vulnerability in the firmware signature checking program of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient checking of an input buffer. An attacker could exploit this vulnerability by passing a crafted file to the affected system. A successful exploit could inhibit an administrator's ability to access the system.

22	CVE-2019-1629	306		2019-06-20	2019-10-09	5.0	None	Remote	Low	Not required	None	Partial	None

A vulnerability in the configuration import utility of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to have write access and upload arbitrary data to the filesystem. The vulnerability is due to a failure to delete temporarily uploaded files. An attacker could exploit this vulnerability by crafting a malicious file and uploading it to the affected device. An exploit could allow the attacker to fill up the filesystem or upload malicious scripts.

23	CVE-2019-1628	191	DoS Overflow	2019-06-20	2021-10-29	2.1	None	Local	Low	Not required	None	None	Partial

A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect bounds checking. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. An exploit could allow the attacker to cause a buffer overflow, resulting in a process crash and DoS condition on the device.

24	CVE-2019-1627	312	+Priv	2019-06-20	2020-10-06	4.0	None	Remote	Low	???	Partial	None	None

A vulnerability in the Server Utilities of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to gain unauthorized access to sensitive user information from the configuration data that is stored on the affected system. The vulnerability is due to insufficient protection of data in the configuration file. An attacker could exploit this vulnerability by downloading the configuration file. An exploit could allow the attacker to use the sensitive information from the file to elevate privileges.

25	CVE-2018-0431	77	Exec Code	2018-10-05	2019-10-09	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with root privileges on an affected device. The vulnerability is due to insufficient validation of command input by the affected software. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to inject and execute arbitrary, system-level commands with root privileges on an affected device.

26	CVE-2018-0430	77	Exec Code	2018-10-05	2019-10-09	9.0	None	Remote	Low	???	Complete	Complete	Complete

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with root privileges on an affected device. The vulnerability is due to insufficient validation of command input by the affected software. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to inject and execute arbitrary, system-level commands with root privileges on an affected device.

27	CVE-2018-0338	863	Exec Code	2018-06-07	2020-09-04	4.6	None	Local	Low	Not required	Partial	Partial	Partial

A vulnerability in the role-based access-checking mechanisms of Cisco Unified Computing System (UCS) Software could allow an authenticated, local attacker to execute arbitrary commands on an affected system. The vulnerability exists because the affected software lacks proper input and validation checks for certain file systems. An attacker could exploit this vulnerability by issuing crafted commands in the CLI of an affected system. A successful exploit could allow the attacker to cause other users to execute unwanted arbitrary commands on the affected system. Cisco Bug IDs: CSCvf52994.

28	CVE-2017-12341	77	Exec Code	2017-11-30	2019-10-09	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in the CLI of Cisco NX-OS System Software could allow an authenticated, local attacker to perform a command injection attack. An attacker would need valid administrator credentials to perform this exploit. The vulnerability is due to insufficient input validation during the installation of a software patch. An attacker could exploit this vulnerability by installing a crafted patch image with the vulnerable operation occurring prior to patch activation. An exploit could allow the attacker to execute arbitrary commands on an affected system as root. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 2000 Series Fabric Extenders, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Unified Computing System Manager. Cisco Bug IDs: CSCvf23735, CSCvg04072.

29	CVE-2017-12338	20		2017-11-30	2019-10-09	2.1	None	Local	Low	Not required	Partial	None	None

A vulnerability in the CLI of Cisco NX-OS System Software could allow an authenticated, local attacker to read the contents of arbitrary files. The vulnerability is due to insufficient input validation for a specific CLI command. An attacker could exploit this vulnerability by issuing a crafted command on the CLI. An exploit could allow the attacker unauthorized access to read arbitrary files on the underlying local file system. On products that support multiple virtual device contexts (VDCs), this vulnerability could allow an attacker to read files from any VDC. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 2000 Series Fabric Extenders, Nexus 3000 Series Switches, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode, Nexus 9000 Series Switches in standalone NX-OS mode, Nexus 9500 R-Series Line Cards and Fabric Modules, Unified Computing System Manager. Cisco Bug IDs: CSCve51707, CSCve93961,

CSCve93964, CSCve93965, CSCve93968, CSCve93974, CSCve93976.

30	CVE-2017-12336	20	Exec Code +Priv	2017-11-30	2017-12-15	4.6	None	Local	Low	Not required	Partial	Partial	Partial

A vulnerability in the TCL scripting subsystem of Cisco NX-OS System Software could allow an authenticated, local attacker to escape the interactive TCL shell and gain unauthorized access to the underlying operating system of the device. The vulnerability exists due to insufficient input validation of user-supplied files passed to the interactive TCL shell of the affected device. An attacker could exploit this vulnerability to escape the scripting sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user. To exploit this vulnerability, an attacker must have local access and be authenticated to the targeted device with administrative or tclsh execution privileges. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 2000 Series Fabric Extenders, Nexus 3000 Series Switches, Nexus 3500 Platform Switches, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode, Nexus 9500 R-Series Line Cards and Fabric Modules, Unified Computing System Manager. Cisco Bug IDs: CSCve93750, CSCve93762, CSCve93763, CSCvg04127.

31	CVE-2017-12335	77	Exec Code +Priv	2017-11-30	2019-10-03	4.6	None	Local	Low	Not required	Partial	Partial	Partial

A vulnerability in the CLI of Cisco NX-OS System Software could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command and gain unauthorized access to the underlying operating system of the device. An exploit could allow the attacker to execute arbitrary commands at the user's privilege level. On products that support multiple virtual device contexts (VDCs), this vulnerability could allow an attacker to execute commands at the user's privilege level outside the user's environment. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 2000 Series Fabric Extenders, Nexus 3000 Series Switches, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode, Nexus 9500 R-Series Line Cards and Fabric Modules, Unified Computing System Manager. Cisco Bug IDs: CSCvf14923, CSCvf14926, CSCvg04095.

32	CVE-2017-12334	20	Exec Code	2017-11-30	2017-12-15	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in the CLI of Cisco NX-OS System Software could allow an authenticated, local attacker to perform a command injection attack. An attacker would need valid administrator credentials to perform this exploit. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to execute arbitrary commands as root. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 2000 Series Fabric Extenders, Nexus 3000 Series Switches, Nexus 3500 Platform Switches, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode, Nexus 9500 R-Series Line Cards and Fabric Modules, Unified Computing System Manager. Cisco Bug IDs: CSCvf15113, CSCvf15122, CSCvf15125, CSCvf15131, CSCvf15143, CSCvg04088.

33	CVE-2017-12333	347	Bypass	2017-11-30	2017-12-15	4.6	None	Local	Low	Not required	Partial	Partial	Partial

A vulnerability in Cisco NX-OS System Software could allow an authenticated, local attacker to bypass signature verification when loading a software image. The vulnerability is due to insufficient NX-OS signature verification for software images. An authenticated, local attacker could exploit this vulnerability to bypass signature verification and load a crafted, unsigned software image on a targeted device. The attacker would need valid administrator credentials to perform this exploit. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Unified Computing System Manager. Cisco Bug IDs: CSCvf25045, CSCvf31495.

34	CVE-2017-12332	434		2017-11-30	2017-12-15	4.9	None	Local	Low	Not required	None	Complete	None

A vulnerability in Cisco NX-OS System Software patch installation could allow an authenticated, local attacker to write a file to arbitrary locations. The vulnerability is due to insufficient restrictions in the patch installation process. An attacker could exploit this vulnerability by installing a crafted patch image on an affected device. The vulnerable operation occurs prior to patch activation. An exploit could allow the attacker to write arbitrary files on an affected system as root. The attacker would need valid administrator credentials to perform this exploit. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 2000 Series Fabric Extenders, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Unified Computing System Manager. Cisco Bug IDs: CSCvf16513, CSCvf23794, CSCvf23832.

35	CVE-2017-12331	347	Bypass	2017-11-30	2017-12-15	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in Cisco NX-OS System Software could allow an authenticated, local attacker to bypass signature verification when loading a software patch. The vulnerability is due to insufficient NX-OS signature verification for software patches. An authenticated, local attacker could exploit this vulnerability to bypass signature verification and load a crafted, unsigned software patch on a targeted device. The attacker would need valid administrator credentials to perform this exploit. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Unified Computing System Manager. Cisco Bug IDs: CSCvf16494, CSCvf23655.

36	CVE-2017-12329	77	Exec Code	2017-11-30	2019-10-09	4.6	None	Local	Low	Not required	Partial	Partial	Partial

A vulnerability in the CLI of Cisco Firepower Extensible Operating System (FXOS) and NX-OS System Software could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation of command arguments to the CLI parser. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to execute arbitrary commands at the user's privilege level. On products that support multiple virtual device contexts (VDCs), this vulnerability could allow the attacker to execute commands at the user's privilege level outside the user's environment. This vulnerability affects the following products running Cisco FXOS or NX-OS System Software: Firepower 4100 Series Next-Generation Firewall, Firepower 9300 Security Appliance, Multilayer Director Switches, Nexus 1000V Series Switches, Nexus 2000 Series Fabric Extenders, Nexus 3000 Series Switches, Nexus 3500 Platform Switches, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode, Nexus 9500 R-Series Line Cards and Fabric Modules, Unified Computing System Manager. Cisco Bug IDs: CSCve51700, CSCve93833, CSCve93860, CSCve93863, CSCve93864, CSCve93880.

37	CVE-2017-6604	601		2017-04-07	2017-07-12	5.8	None	Remote	Medium	Not required	Partial	Partial	None

A vulnerability in the web interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to

redirect a user to a malicious web page. This vulnerability affects the following Cisco products running Cisco IMC Software: Unified Computing System (UCS) B-Series M3 and M4 Blade Servers, Unified Computing System (UCS) C-Series M3 and M4 Rack Servers. More Information: CSCvc37931. Known Affected Releases: 3.1(2c)B.

38	CVE-2017-6602	78		2017-04-07	2019-10-03	3.6	None	Local	Low	Not required	Partial	Partial	None

A vulnerability in the CLI of Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb66189 CSCvb86775. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1742) 92.1(1.1658) 2.1(1.38) 2.0(1.107) 2.0(1.87) 1.1(4.148) 1.1(4.138).

39	CVE-2017-6601	78		2017-04-07	2019-10-03	3.6	None	Local	Low	Not required	Partial	Partial	None

A vulnerability in the CLI of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61384 CSCvb86764. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1647).

40	CVE-2017-6600	78		2017-04-07	2019-10-03	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in the CLI of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61351 CSCvb61637. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1645) 2.0(1.82) 1.1(4.136.

41	CVE-2017-6598	862	Exec Code	2017-04-07	2019-10-03	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in the debug plug-in functionality of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to execute arbitrary commands, aka Privilege Escalation. More Information: CSCvb86725 CSCvb86797. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.105) 92.1(1.1733) 2.1(1.69).

42	CVE-2017-6597	78		2017-04-07	2017-07-12	7.2	None	Local	Low	Not required	Complete	Complete	Complete

A vulnerability in the local-mgmt CLI command of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61394 CSCvb86816. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1658) 2.0(1.115).

43	CVE-2016-6402	264		2016-09-18	2017-07-30	7.2	None	Local	Low	Not required	Complete	Complete	Complete

UCS Manager and UCS 6200 Fabric Interconnects in Cisco Unified Computing System (UCS) through 3.0(2d) allow local users to obtain OS root access via crafted CLI input, aka Bug ID CSCuz91263.

44	CVE-2015-6435	78	Exec Code	2016-01-22	2021-01-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An unspecified CGI script in Cisco FX-OS before 1.1.2 on Firepower 9000 devices and Cisco Unified Computing System (UCS) Manager before 2.2(4b), 2.2(5) before 2.2(5a), and 3.0 before 3.0(2e) allows remote attackers to execute arbitrary shell commands via a crafted HTTP request, aka Bug ID CSCur90888.

45	CVE-2015-6355	200	+Info	2015-11-04	2018-10-30	5.0	None	Remote	Low	Not required	Partial	None	None

The web interface in Cisco Unified Computing System (UCS) 2.2(5b)A on blade servers allows remote attackers to obtain potentially sensitive version information by visiting an unspecified URL, aka Bug ID CSCuw87226.

46	CVE-2015-4279	78	+Priv	2015-07-20	2017-09-22	7.2	None	Local	Low	Not required	Complete	Complete	Complete

The Manager component in Cisco Unified Computing System (UCS) 2.2(3b) on B Blade Server devices allows local users to gain privileges for executing arbitrary CLI commands by leveraging access to the subordinate fabric interconnect, aka Bug ID CSCut32778.

47	CVE-2015-4259	310	Bypass	2015-07-10	2016-12-28	4.3	None	Remote	Medium	Not required	Partial	None	None

The Integrated Management Controller on Cisco Unified Computing System (UCS) C servers with software 1.5(3) and 1.6(0.16) has a default SSL certificate, which makes it easier for man-in-the-middle attackers to bypass cryptographic protection mechanisms by leveraging knowledge of a private key, aka Bug IDs CSCum56133 and CSCum56177.

48	CVE-2015-4183	78	Exec Code +Priv	2015-06-17	2016-12-07	7.2	None	Local	Low	Not required	Complete	Complete	Complete

Cisco UCS Central Software 1.2(1a) allows local users to gain privileges for OS command execution via a crafted CLI parameter, aka Bug ID CSCut32795.

49	CVE-2015-0718	399	DoS	2016-03-03	2016-12-03	7.8	None	Remote	Low	Not required	None	None	Complete

Cisco NX-OS 4.0 through 6.1 on Nexus 1000V 3000, 4000, 5000, 6000, and 7000 devices and Unified Computing System (UCS) platforms allows remote attackers to cause a denial of service (TCP stack reload) by sending crafted TCP packets to a device that has a TIME_WAIT TCP session, aka Bug ID CSCub70579.

50	CVE-2014-8009	200	+Info	2014-12-10	2015-01-24	5.0	None	Remote	Low	Not required	Partial	None	None

The Management subsystem in Cisco Unified Computing System 2.1(3f) and earlier allows remote attackers to obtain sensitive information by reading log files, aka Bug ID CSCur99239.

Total number of vulnerabilities : **53** Page : 1 (This Page) 2

How does it work? Known limitations & technical details User agreement, disclaimer and privacy statement About & Contact Feedback