	# CVE ID CWE ID # of	f Exploits Vulnerability Type(s)	Publish Date U	pdate Date Sc	core Access Complexity	
1						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
Major Majo	1 CVF 2024 44220 44220	20 Even Code	12/10/2021	4/2/2022	0.2 Domesto Medium	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
1	1 CVE-2021-44228 44228	20 Exec Code	12/10/2021	4/3/2023	9.3 Remote Medium	
Part	2 CVE-2020-10136 10136	290 Bypass	6/2/2020	7/29/2020	5 Remote Low	
Procession Pro						
A MARINE SIGN BIT SIG	3 CVF-2019-1966 1966	Exec Code +Priv	8/30/2019	10/16/2020	7.2 Local Low	
	3 601 2019 1900 1900	LACO COUC IT III	5/50/2013	10/ 10/ 1020	7.2 2000. 2011	
A Proposition of the Proposition						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
Set 1991 18 1	4 CVE-2019-1908 1908		8/21/2019	10/16/2020	5 Remote Low	•
1						
Column C	5 CVE-2019-1907 1907	+Priv	8/21/2019	10/16/2020	6.5 Remote Low	
Control Cont						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
A considerability in the architecture control and of the control o	C CVE 2010 1000 1000	47C DeC	0/21/2010	2/24/2022	7.0 Domete Jaw	
Part	6 CVE-2019-1900 1900	476 DOS	8/21/2019	3/31/2023	7.8 Remote Low	
1						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
A consequency control (Count Dougle and Section 1) (Count Dougle and Secti						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
## Application of the Company of the	7 CVE-2019-1896 1896	78 Exec Code	8/21/2019	3/31/2023	9 Remote Low	
Control 2015 18 18 18 18 18 18 18						
4 subsectivity in the command of interface of Concurrency and Engineer Control (PME) coult allows an attender control (PME) coult allow	8 CVE-2019-1885 1885	78 Exec Code	8/21/2019	3/31/2023	9 Remote Low	
Section 1987						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
Procession Pro						
A uniconstantly in the CI Lot Citcus integrate Management Controller (MQC) could allow an autheritecting with the demandating of the anti-ordinal type of the CI and Citcus integrated Security Association and a security of the anti-ordinal security of the se	0 CVE 2010 1992 1992	79 Evec Code	9/21/2010	2/21/2022	7.2 Local Low	
whereboth to the considerate valuation of our supplied part at the C1. As attacker could exploy this value analysing by attackets dright of the administratory personals of the C1 and analysing the country of the C1. As attacker could as only attackers of a second as a full country of the analysing the country of the analysing the country of the coun	9 CVE-2019-1883	76 Exec Code	6/21/2019	3/31/2023	7.2 LOCAL LOW	
A value-rability of the integrated Management Controller (MAC) could allow as authenticating, premise at section of except and implement and integrated sharpes more controller (MAC) could allow as authenticating, premise at section of except and implement and implement and interval of the implement and implem						
and implement with the part and interpretation places are neglected educes. The value regulation packed to an artificide educine. The value regulation packed are presented an experiation butter for educine packed and present an artificide educine. The value regulated butter packed as presented and packed packed and packed an experiation packed and packed packed and packed packed. The value regulated butter packed and packed packed packed and packed packed packed and packed	10 CVE-2019-1879 1879	78 Exec Code	6/20/2019	10/9/2019	7.2 Local Low	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.
Manual Published Manual Publ						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
1 (17 10 10 00 00 00 00 00 00 00 00 00 00 00						
A value command, with configuration than the second another interface of Custo Integrated Management Controller (IMC) Software could allow an authenticated, errors attacker to Inject and tractice could exploit to without allow an authenticated, errors attacker to Inject and executed within rough in interface monitoring mechanisms with a cripidal agruement on the affected software. As scientific application in the value of the property of the second allow the attacker to Inject and execute arbitrary, yettern-level commands that is executed within 10 miles and interface and ordered device. 12 CVF-2019-1809 1864 78 Exec Code 8/11/2019 3/11/2023 9 Remote 10 miles and the second arbitrary of the second device. The value and the second device in the value and the second device. The value and the second device in the value and the second device in the value and the second device. The value and the second device in the value and the second device. The value and the second device in the value and the second device in the value and the second device. The value and the second device in the value and the second device. The value and the second device in the value and the second device. The value and the second device in the value and the second device. The value and the second device in the value and the val	11 CVE-2019-1871 1871	119 DoS Overflow	8/21/2019	10/9/2019	9 Remote Low	
1 Note 2				-,-,-		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
12 CPC 2019-1885 1855 78 Exec Code 8 (71/2019 31/2022) 9 February 1 (1994) 1879 1879 1879 1879 1879 1879 1879 1879						
A valuescability in the web-based management interface of Class integrated Management. Countroller [MC], Software could allow an authenticated, remote attacker to original time values of the property of the country o	12 CVF 2010 1965 1965	70 Even Code	9/21/2010	2/21/2022	O Domoto Lour	
secuted with root privileges on an affected device. The vulnerability is use to instifficient validation of command input by the affected software. An attacker could exploit this vulnerability by sending a crafted stream. A successful replication deliver the end of privileges on an affected device. 12 (VE-2019-186) 18-4 78 Evec Code 8/21/2019 10/16/2029 9 Remote	12 CVE-2019-1805 1805	78 Exec Code	8/21/2019	3/31/2023	9 Remote Low	
12 CVF-2019-1865 18-6 18						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
A volume bility in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to make unsubtraised danges to the affected oblivers. A volume bility in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to make unsubtraised on engagement. The valume bility is the web-based management controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that in exception of the developer injection of the value of the						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-
system configuration. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by sending a crited HTTP request to the affected downs. A successful exploit could allow as use with read-only privileges to change critical system configurations using administrator privileges. A vulnerability in the web-based management instration of close or the grant affect of social system configurations using administrator privileges. A sunface of close to integrated Management. Centroller (MIC) Software could allow an authenticated, remote attacker to inject and retacker with elevated privileges to change critical system configurations using administrator or redeministrator representations. The vulnerability is due to insufficient authorization closely as the controller (MIC) Software could allow an authenticated, remote attacker to inject and execute authorizacy, system-level commands to the administrator representation to the administrator representation of the administrator repre	13 CVE-2019-1864 1864	78 Exec Code	8/21/2019	3/31/2023	9 Remote Low	
14 CVE-2019-1863 1863 - 8/12/020 10/16/2020 9 Remote Low successful evaluation could allow a user with read-only privileges to change critical system configurations using administrator privileges. A vulnerability in the web-based management controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that excessful evaluation of users using the controller of the co						
A universibility in the web-based management. Controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that a concusion with root privileges on an affected device. An attacker would need to have could end in how are could allow an authenticated, premote attacker to inject arbitrary commands that a concusion with root privileges on an affected device. An attacker would need to have could exploit this vulnerability by sending crafted commands to the administrative web management interface of the affected software. A vulnerability in the Immune of the Cisco USC Series Rack Servers could allow an authenticated, premote attacker to inject arbitrary commands with root privileges on an affected device. The vulnerability is due to improper validation of the server immune undersity of the server immune undersity in the server immune could allow the attacker to device. The vulnerability is due to improper validation of the server immune undersity in the server immune undersi	14 CVE-2019-1863 1863		8/21/2019	10/16/2020	9 Remote Low	
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. An attacker with elevated privileges on an affected device. The vulnerability by sending crafted commands with root privileges on an affected device. A vulnerability of the commands. As a volnerability of the commands with root privileges on an affected device. A vulnerability of the commands with root privileges on an affected device. A vulnerability of the commands with root privileges on an affected device. A vulnerability of the commands with root privileges on the affected device. A vulnerability of the vulnerabilit						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
15 CVE-2019-189 1850 78 Exec Code 8/21/2019 10/9/2019 9 Remote Low successful exploit could allow the attacker to niject and execute arbitrary, system-level commands with root privileges on an affected device. The vulnerability is the to improper validation of the server to papsas Unified Extensible Firmware Interface (UEFI) Secure Boot tending this vulnerability by 16 CVE-2019-1736 1736 347 Bypass 9/23/202 10/23/202 54. In CVE-2019-1736 1736 347 Bypass 9/23/202 54. In CVE-2019-1736 34. In CVE-2019-1736 34. In CVE-2019-1736 34. In CVE-2019-1736						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
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 chan and load a compromised software image on an affected device. The vulnerability is due to improper validation of the server firmware vegrated device. The vulnerability is due to improper validation of the server firmware upgrated device. The vulnerability is due to improper validation of the server firmware vegrated device. The vulnerability is due to improper validation of the server firmware vegrated device. A compromised software image on the affected device. A compromised software image on the affected device. A compromised software image is any software image. An attacker could exploit this vulnerability is observed to company in the properties of the properties of the server immands and attacker could exploit this vulnerability by authenticating to the device and issuing a crafted form of a limited subset of local management of the properties of the server immand and an authenticated in the properties of the properties of the server immand and an authenticated in the properties of the server immand and an authenticated in the properties of the server immand and an authenticated in the properties of the server immand an authenticated in the properties of the server immand and an auth	15 CVE 2010 1950 1950	79 Evec Code	9/21/2010	10/0/2010	O Romoto Low	
and load a compromised offware 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 UEF Secure Boot. A successful exploit could allow the attacker to disable UEF Secure Boot. A successful exploit could allow the attacker to disable UEF Secure Boot. A successful exploit could allow the attacker to disable UEF Secure Boot. A successful exploit could allow the attacker to disable UEF Secure Boot. A successful exploit could allow the attacker to depend on the discount of the server firmware upgrade images. An attacker could input manual to the server firmware upgrade images. An attacker could input manual and the server firmware upgrade images. An attacker could lead to a successful exploit could allow the attacker to depend on the discount of several proposed of the server firmware upgrade images. An attacker could input manual exploit and understanced on the server firmware upgrade images. An attacker could allow the attacker to specific commands on the Cisco UCS 8-series Blade Servers could allow an authenticated, local attacker to or disable. Understanding to the device and issuing a carted form of a limited subset of local management CLL commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a carted form of a limited subset of local management and understanced understanced to prove version 4.0(2a) and atter. Yes 78 Yes 8 Exec Code + Priv 8/12/101 9 10/16/202 9 8 Permit Valuerability in the intelligent Platform Management Interface (IPMI) of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to opain rotted with corporating system (OS). The vulnerability is due to insufficient input validation of user-supplied commands. An attacker to gain rotted with corporating version to exploit this vulnerability by submitting crafted input to the affec	15 CVE-2019-1850 1850	78 Exec Code	8/21/2019	10/9/2019	9 Remote Low	
16 CVE-2019-1736 1736 347 Bypass 9/23/2020 10/23/2020 6.9 Local Medium Secure Boot technology and load a compromised software image on the affected device. A compromised software image is any software image in the Cisc out Sc Sc Sc Sie Bode Screes Could allow an authenticated, local attacker to oke whether special device. A compromised software image is any software image in the Cisc out Sc						
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 of disk. it is also possible the attacker could engernet CLI commands. An attacker could engernet CLI commands. The vulnerability is fixed in an agement CLI commands. An exploit could allow the 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 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. A vulnerability in the Intelligent Platform Management Interface (IPMI) of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker who has a administrator privileges on the underlying operating system (OS). The vulnerability is due to insufficient input validation of user-supplied commands. An attacker who has a administrator privileges and access to the network where the IPMI resides could exploit this vulnerability by submitting crafted input to the affected commands. An accessful exploit could allow an authenticated, remote attacker to ogain root privileges on the affected device. 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 attacks) and perform arbitrary actions on an affected device. A 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 a larkefeted device. For the v						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 UEF
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 limitled subset of local management CLI commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a crafted form of a limitled subset of local management CLI commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a crafted form of a limitled subset of local management CLI commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a crafted form of a limitled subset of local management CLI commands and the device and issuing a crafted form of a limitled subset of local management CLI commands and the device and issuing a crafted form of a limitled subset of local management CLI commands and the device and issuing a crafted form of a limitled subset of local management cLI commands and the device and issuing a crafted form of a limitled subset of local management cLI commands and the device and issuing a crafted form of a limitled subset of local management cLI commands and the subset of local management clief to exploit this vulnerability in the left and the converting and the con	16 CVE-2019-1736 1736	347 Bypass	9/23/2020	10/23/2020	6.9 Local Medium	
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 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. 8 VE-2019-1634 1634 78 Exec Code +Priv 8/21/2019 10/16/202 9 Remote 1.0 Exec Code +Priv 8/21/2019 10/16/202 9 Remote 1						
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. 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. 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. 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 attack and perform arbitrary actions on an affected device. 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. A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on a flected device. A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on a flected device. A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on a flected device. A vulnerability in the web-based management interface of Cisco Integrated						
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 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. 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 allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on a feeted device. 19 CVE-2019-1632 1632 352 CSRF 6/20/2019 10/9/2019 6 Remote Wed-based management interface of Cisco Integrated Management Controller (IMC) could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on the affected device. 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						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
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. 8 21/2019 10/16/2020 9 Remote	17 CVE-2019-1725 1725	78	4/18/2019	10/8/2020	3.6 Local Low	V 7
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. 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 a flected device. 19 CVE-2019-1632 1632 352 CSRF 6/20/2019 10/9/2019 6 Remote 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						
18 CVE-2019-1634 1634 78 Exec Code +Priv 8/21/2019 10/16/2020 9 Remote Low root privileges on the affected device. 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 a flected device. 19 CVE-2019-1632 1632 352 CSRF 6/20/2019 10/9/2019 6 Remote Medium the affected device. 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						
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. 19 CVE-2019-1632 1632 352 CSRF 6/20/2019 10/9/2019 6 Remote Medium the affected device. 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	18 CVE-2019-1634 1634	78 Exec Code +Priv	8/21/2019	10/16/2020	9 Remote Low	
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 of the user to perform arbitrary action						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)
19 CVE-2019-1632 1632 352 CSRF 6/20/2019 10/9/2019 6 Remote Medium the affected device. 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						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
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	19 CVF-2019-1632 1622	352 CSRF	6/20/2010	10/9/2010	6 Remote Medium	
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	13 CAT 5013-1035 1035	JJZ CJNI	0/ 20/ 2019	10/3/2013	o nemote ivieuluiii	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
20 CVE-2019-1631 1631 306 6/20/2019 10/9/2019 5 Remote Low exploit could allow an attacker to view sensitive system data.						
	20 CVE-2019-1631 1631	306	6/20/2019	10/9/2019	5 Remote Low	exploit could allow an attacker to view sensitive system data.

						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
21 CVE-2019-1630 1630	110 Dos Overflow Bypass	6/20/2010 10/0	9/2019	2.1 Local	Low	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.
21 CVE-2019-1030 1630	119 DoS Overflow Bypass	6/20/2019 10/9	9/2019	Z.1 LUCAI	Low	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
22 CVE-2019-1629 1629	306	6/20/2019 10/9	9/2019	5 Remote	Low	exploit could allow the attacker to fill up the filesystem or upload malicious scripts.
						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
23 CVE-2019-1628 1628	191 DoS Overflow	6/20/2019 10/29	9/2021	2.1 Local	Low	the attacker to cause a buffer overflow, resulting in a process crash and DoS condition on the device.
		•	•			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
		2/22/22/2	- 1			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
24 CVE-2019-1627 1627	312 #NAME?	6/20/2019 10/6	6/2020	4 Remote	e Low	configuration file. An exploit could allow the attacker to use the sensitive information from the file to elevate privileges. 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
25 CVE-2018-0431 0431	77 Exec Code	10/5/2018 10/9	9/2019	9 Remote	Low	privileges on an affected device.
						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
26 CVE-2018-0430 0430	77 Exec Code	10/5/2018 10/9	9/2019	9 Remote	e Low	privileges on an affected device.
						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
27 CVE-2018-0338 0338	863 Exec Code	6/7/2018 9/4	4/2020	4.6 Local	Low	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:
27 CVE-2018-0338 0338	803 Exec Code	0/7/2016 3/2	4/2020	4.0 LOCal	LOW	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
28 CVE-2017-12341 12341	77 Exec Code	11/30/2017 10/9	9/2019	7.2 Local	Low	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.
20 CVE-2017-12341 12341	77 Exec Code	11/30/2017 10/5	3/2013	7.2 LUCai	LOW	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 7000 Series Switches, Nexus 7000 Series Switches, Nexus 700 Series Switches, Nexus 7000
						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,
29 CVE-2017-12338 12338	20	11/30/2017 10/9	9/2019	2.1 Local	Low	CSCve93965, CSCve93968, CSCve93974, CSCve93976.
						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 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-
30 CVE-2017-12336 12336	20 Exec Code +Priv	11/30/2017 12/15	5/2017	4.6 Local	Low	Series Line Cards and Fabric Modules, Unified Computing System Manager. Cisco Bug IDs: CSCve93750, CSCve93762, CSCve93763, CSCve93763, CSCvg04127.
						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 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000
31 CVE-2017-12335 12335	77 Exec Code +Priv	11/30/2017 10/3	3/2019	4.6 Local	Low	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.
31 672 2017 12333 12333	77 Exec code 1111	11/30/2017 10/5	3,2013	1.0 Local	2011	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
32 CVE-2017-12334 12334	20 Exec Code	11/30/2017 12/15	5/2017	7.2 Local	Low	Computing System Manager. Cisco Bug IDs: CSCvf15113, CSCvf15122, CSCvf15131, CSCvf15131, CSCvf15143, CSCvg04088.
						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
33 CVE-2017-12333 12333	347 Bypass	11/30/2017 12/15	5/2017	4.6 Local	Low	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.
12 212 222. 22300 12300	, - , - , - , - , - , - , - , - , -	,,,	-,= v= ,		=•••	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
34 CVE-2017-12332 12332	434	11/30/2017 12/15	5/2017	4.9 Local	Low	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 Switc
3. 3.2 201, 12002 12002		,00,201, 12,10	-,	20001		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
25 60/5 2047 42224 4255	247.5	44/20/2017	F /2047	721 '	1 -	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
35 CVE-2017-12331 12331	347 Bypass	11/30/2017 12/15	5/2017	7.2 Local	Low	Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Unified Computing System Manager. Cisco Bug IDs: CSCvf16494, CSCvf23655.

					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,
36 CVE-2017-12329 12329	77 Exec Code	11/30/2017	10/9/2019	4.6 Local Low	CSCve93860, CSCve93863, CSCve93864, CSCve93880.
					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
37 CVE-2017-6604 6604	601	4/7/2017	7/12/2017	5.8 Remote Medium	Rack Servers. More Information: CSCvc37931. Known Affected Releases: 3.1(2c)B.
					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)
38 CVE-2017-6602 6602	78	4/7/2017	10/3/2019	3.6 Local Low	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).
					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)
39 CVE-2017-6601 6601	78	4/7/2017	10/3/2019	3.6 Local Low	92.1(1.1647).
					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)
40 CVE-2017-6600 6600	78	4/7/2017	10/3/2019	7.2 Local Low	92.1(1.1645) 2.0(1.82) 1.1(4.136.
					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.
41 CVE-2017-6598 6598	862 Exec Code	4/7/2017	10/3/2019	7.2 Local Low	Known Fixed Releases: 92.2(1.105) 92.1(1.1733) 2.1(1.69).
					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
42 CVE-2017-6597 6597	78	4/7/2017	7/12/2017	7.2 Local Low	Releases: 92.2(1.101) 92.1(1.1658) 2.0(1.115).
43 CVE-2016-6402 6402	264	9/18/2016	7/30/2017	7.2 Local Low	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.
					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
44 CVE-2015-6435 6435	78 Exec Code	1/22/2016	1/30/2021	10 Remote Low	remote attackers to execute arbitrary shell commands via a crafted HTTP request, aka Bug ID CSCur90888.
					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
45 CVE-2015-6355 6355	200 #NAME?	11/4/2015	10/30/2018	5 Remote Low	ID CSCuw87226.
					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
46 CVE-2015-4279 4279	78 #NAME?	7/20/2015	9/22/2017	7.2 Local Low	subordinate fabric interconnect, aka Bug ID CSCut32778.
					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
47 CVE-2015-4259 4259	310 Bypass	7/10/2015	12/28/2016	4.3 Remote Medium	attackers to bypass cryptographic protection mechanisms by leveraging knowledge of a private key, aka Bug IDs CSCum56133 and CSCum56177.
48 CVE-2015-4183 4183	78 Exec Code +Priv	6/17/2015	12/7/2016	7.2 Local Low	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.
					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
49 CVE-2015-0718 0718	399 DoS	3/3/2016	12/3/2016	7.8 Remote Low	reload) by sending crafted TCP packets to a device that has a TIME_WAIT TCP session, aka Bug ID CSCub70579.
50 CVE-2014-8009 8009	200 #NAME?	12/10/2014	1/24/2015	5 Remote Low	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.