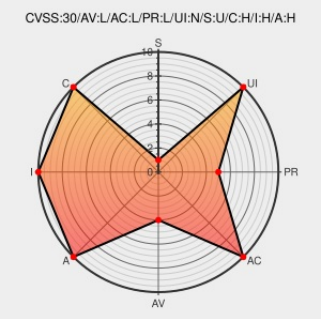
CVE-2020-3171

Published on: 02/26/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3171 - advisory for cisco-sa-20200226-fxos-ucs-cli-cmdinj

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firepower 2110 from Cisco contain the following vulnerability:

A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.

CVE-2020-3171 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Adaptive Security Appliance (ASA) Software** version **n/a**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco FXOS and UCS Manager Software Local Management CLI Command Injection Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200226 Cisco FXOS and UCS Manager Software Local Management CLI Command Injection Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Firepower 2110	-	All	All	All
Hardware	Cisco	Firepower 2110	-	All	All	All
Hardware	Cisco	Firepower 2120	-	All	All	All
Hardware	Cisco	Firepower 2120	-	All	All	All
Hardware	Cisco	Firepower 2130	-	All	All	All
Hardware	Cisco	Firepower 2130	-	All	All	All
Hardware	Cisco	Firepower 2140	-	All	All	All
Hardware	Cisco	Firepower 2140	-	All	All	All
Hardware	Cisco	Firepower 4110	-	All	All	All
Hardware	Cisco	Firepower 4110	-	All	All	All
Hardware	Cisco	Firepower 4115	-	All	All	All
Hardware	Cisco	Firepower 4115	-	All	All	All
Hardware	Cisco	Firepower 4120	-	All	All	All
Hardware	Cisco	Firepower 4120	-	All	All	All
Hardware	Cisco	Firepower 4125	-	All	All	All
Hardware	Cisco	Firepower 4125	-	All	All	All
Hardware	Cisco	Firepower 4140	-	All	All	All
Hardware	Cisco	Firepower 4140	-	All	All	All

Hardware	Cisco	Firepower 4145	-	All	All	All
Hardware	Cisco	Firepower 4145	-	All	All	All
Hardware	Cisco	Firepower 4150	-	All	All	All
Hardware	Cisco	Firepower 4150	-	All	All	All
Hardware	Cisco	Firepower 9300	-	All	All	All
Hardware	Cisco	Firepower 9300	-	All	All	All
Operating System	Cisco	Fxos	2.4\(1.214\)	All	All	All
Operating System	Cisco	Fxos	2.4\(1.216\)	All	All	All
Operating System	Cisco	Fxos	2.4\(1.214\)	All	All	All
Operating System	Cisco	Fxos	2.4\(1.216\)	All	All	All
Hardware	Cisco	Ucs 6248up	-	All	All	All
Hardware	Cisco	Ucs 6248up	-	All	All	All
Hardware	Cisco	Ucs 6296up	-	All	All	All
Hardware	Cisco	Ucs 6296up	-	All	All	All
Hardware	Cisco	Ucs 6324	-	All	All	All
Hardware	Cisco	Ucs 6324	-	All	All	All
Hardware	Cisco	Ucs 6332	-	All	All	All
Hardware	Cisco	Ucs 6332	-	All	All	All
Hardware	Cisco	Ucs 6332-16up	-	All	All	All
Hardware	Cisco	Ucs 6332-16up	-	All	All	All
Hardware	Cisco	Ucs 64108	-	All	All	All
Hardware	Cisco	Ucs 64108	-	All	All	All
Hardware	Cisco	Ucs 6454	-	All	All	All
Hardware	Cisco	Ucs 6454	-	All	All	All
Application	Cisco	Ucs Manager	4.0\(1a\)a	All	All	All
Application	Cisco	Ucs Manager	4.0\(1a\)a	All	All	All

cpe:2.3:h:cisco:firepower_2110:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2110:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2120:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2120:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2130:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2130:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2140:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_2140:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4110:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4110:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4115:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4115:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4120:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4120:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4125:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4125:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4140:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4140:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4145:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4145:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4150:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_4150:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_9300:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:firepower_9300:-:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:fxos:2.4\(1.214\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:fxos:2.4\(1.216\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:fxos:2.4\(1.214\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:fxos:2.4\(1.216\):*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6248up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6248up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6296up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6296up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6324:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6324:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6332:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6332:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6332-16up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6332-16up:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_64108:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_64108:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6454:-:*:*:*:*:*:*:*:

cpe:2.3:h:cisco:ucs_6454:-:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_manager:4.0\(1a\)a:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_manager:4.0\(1a\)a:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report