Cisco Security Advisory

Cisco UCS Manager Software Local Management CLI Command Injection Vulnerability

High

Advisory ID: cisco-sa-20200226-ucs-cli-cmdinj

First Published: 2020 February 26 16:00 GMT

Version 1.0: Final

CVE-2020-3173

Workarounds: No workarounds available

Cisco Bug IDs: CSCvq57926

CVSS Score:
Base 7.8

Download CSAF Download CVRF Email

Summary

A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device.

The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. 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.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-ucs-cli-cmdinj

This advisory is part of the February 2020 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication, which includes six Cisco Security Advisories that describe six vulnerabilities. For a complete list of the advisories and links to them, see Cisco Event Response: February 2020 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication.

Affected Products

Vulnerable Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco UCS Manager Software:

- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- MDS 9000 Series Multilayer Switches
- Nexus 1000 Virtual Edge for VMware vSphere
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 Series Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode

- Nexus 9000 Series Switches in standalone NX-OS mode

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license:
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco TAC:
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Cisco UCS Software

In the following table(s), the left column lists Cisco software releases. The center column indicates whether a release is affected by the vulnerability described in this advisory and the first release that includes the fix for this vulnerability. The right column indicates whether a release is affected by all the vulnerabilities described in this bundle and which release includes fixes for those vulnerabilities.

UCS 6200, 6300, and 6400 Series Fabric Interconnects: CSCvq57926

Cisco UCS Software Release	First Fixed Release for This Vulnerability	First Fixed Release for All Vulnerabilities Described in the Bundle of Advisories
Earlier than 3.2	Migrate to a fixed release.	Migrate to a fixed release.
3.2	3.2(3n)	3.2(3n)
4.0	4.0(4c)	4.0(4g)
4.1	Not vulnerable.	Not vulnerable.

Additional Resources

For help determining the best Cisco NX-OS Software release for a Cisco Nexus Switch, administrators can refer to the following Recommended Releases documents. If a security advisory recommends a later release, Cisco recommends following the advisory guidance.

- Cisco MDS Series Switches
- Cisco Nexus 1000V for VMware Switch
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 5500 Platform Switches
- Cisco Nexus 5600 Platform Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 Series Switches
- Cisco Nexus 9000 Series ACI-Mode Switches

To determine the best release for Cisco UCS, see the Recommended Releases documents in the release notes for the device.

Exploitation and Public Announcements

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.

Source

This vulnerability was found by Nikhil Sagotiya of Cisco during internal security testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-ucs-cli-cmdinj

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2020-February-26
