Cisco Security Advisory

Cisco HyperFlex HX Command Injection Vulnerabilities

Advisory ID:	cisco-sa-hyperflex-rce-TjjNrkpR
First Published:	2021 May 5 16:00 GMT
Last Updated:	2022 December 15 22:19 GMT
Version 1.2:	Final
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCvx36014 CSCvx36019 CSCvx37435
CVSS Score:	Base 9.8
	CVE-2021-1497 CVE-2021-1498

Download CSAF Download CVRF Email

Summary

Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device.

For more information about these vulnerabilities, see the Details section of this advisory.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

This advisory is available at the following link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Action Links for This Advisory

Snort Rule 57529

Snort Rule 57531

Snort Rule 57530

Snort Rule 57526

Snort Rule 57528

Related to This Advisory

Your Rating:

Average Rating:

Affected Products

Vulnerable Products

These vulnerabilities affect Cisco devices if they are running a vulnerable release of Cisco HyperFlex HX Software.

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 these vulnerabilities.

Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit the other vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerability.

Details about the vulnerabilities are as follows:

CVE-2021-1497: Cisco HyperFlex HX Installer Virtual Machine Command Injection Vulnerability

A vulnerability in the web-based management interface of Cisco HyperFlex HX Installer Virtual Machine could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the *root* user.

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

Bug ID(s): CSCvx36014, CSCvx36019
CVE ID: CVE-2021-1497

Security Impact Rating (SIR): Critical
CVSS Base Score: 9.8
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2021-1498: Cisco HyperFlex HX Data Platform Command Injection Vulnerability

A vulnerability in the web-based management interface of Cisco HyperFlex HX Data Platform could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the *tomcat8* user.

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

Bug ID(s): CSCvx37435
CVE ID: CVE-2021-1498
Security Impact Rating (SIR): High
CVSS Base Score: 7.3
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Workarounds

There are no workarounds that address these vulnerabilities.

Fixed Software

Cisco has released free software updates that address the vulnerabilities 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 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.

Fixed Releases

In the following table(s), the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerabilities described in this advisory and the first release that includes the fix for these vulnerabilities. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

Cisco HyperFlex HX Release	First Fixed Release
Earlier than 4.0	Migrate to 4.0(2e)
4.0	4.0(2e)
4.5	4.5(2a)

Exploitation and Public Announcements

In November 2021, the Cisco Product Security Incident Response Team (PSIRT) became aware of additional attempted exploitation of this vulnerability in the wild. Cisco continues to strongly recommend that customers upgrade to a fixed software release to remediate this vulnerability.

Source

Cisco would like to thank Nikita Abramov and Mikhail Klyuchnikov of Positive Technologies for reporting these vulnerabilities.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR

Revision History

Version	Description	Section	Status	Date
1.2	Updated exploitation information.	Exploitation and Public Announcements Section	Final	2022-DEC-15
1.1	Corrected the First Fixed Release for the 4.5 release.	Fixed Releases	Final	2021-MAY-07

Show Complete History...
