Cisco Security Advisory

Multiple Vulnerabilities in Cisco UCS Director and Cisco UCS Director Express for Big Data

Advisory ID: cisco-sa-ucsd-mult-vulns-UNfpdW4E

First Published: 2020 April 15 16:00 GMT

Last Updated: 2020 April 17 19:27 GMT

CVE-2020-3239
CVE-2020-3240
CVE-2020-3243
More...

Version 1.1: Final

Workarounds: No workarounds available

Cisco Bug IDs: CSCvs53493
CSCvs53496
CSCvs53500
More...

CVSS Score: Base 9.8

Download CSAF Download CVRF Email

Summary

Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on 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.

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 53671
Snort Rule 53672
Snort Rule 53673
Snort Rule 53674
Snort Rule 53675
Snort Rule 53676
Snort Rule 53677
Snort Rule 53678
Snort Rule 53679
Snort Rule 53680
Show All 11...

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsd-mult-vulns-UNfpdW4E

Affected Products

Vulnerable Products

The following table lists Cisco products that are affected by one or more of the vulnerabilities that are described in this advisory:

Product	Cisco Bug IDs	Vulnerable Release(s)	Fixed Release
Cisco UCS Director	CSCvs53496, CSCvs53493 CSCvs53500, CSCvs53502 CSCvs56400, CSCvs56401 CSCvs56399, CSCvs69171 CSCvs69022	6.0.0.0, 6.0.0.1, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.0.1.3 6.5.0.0, 6.5.0.1, 6.5.0.2, 6.5.0.3, 6.5.0.4 6.6.0.0, 6.6.1.0, 6.6.2.0 6.7.0.0, 6.7.1.0, 6.7.2.0, 6.7.3.0	6.7.4.0
Cisco UCS Director Express for Big Data	CSCvt39561, CSCvt39555 CSCvt39580, CSCvt39565 CSCvt39535, CSCvt39526 CSCvt39575, CSCvt39489	3.7.3.0 and earlier	3.7.4.0

Products Confirmed Not Vulnerable

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

Details

Vulnerability Details

Details about the vulnerabilities are as follows.

Cisco UCS Director and UCS Director Express for Big Data Authentication Bypass Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device.

The vulnerability is due to insufficient access control validation. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit could allow the attacker to interact with the REST API with administrative privileges.

Bug ID(s): CSCvs53496, CSCvt39580
CVE ID: CVE-2020-3243
Security Impact Rating (SIR): Critical
CVSS Base Score: 9.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Cisco UCS Director and UCS Director Express for Big Data Remote Code Execution Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an authenticated, remote attacker to execute arbitrary code with *root* privileges on the underlying operating system.

The vulnerability is due to improper input validation. An attacker could exploit this vulnerability by crafting a malicious file and sending it to the REST API. A successful exploit could allow the attacker to open a remote shell and execute code with *root* privileges.

Bug ID(s): CSCvs56399, CSCvt39555
CVE ID: CVE-2020-3240
Security Impact Rating (SIR): High
CVSS Base Score: 8.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Cisco UCS Director and UCS Director Express for Big Data Authentication Bypass Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an unauthenticated, remote attacker to bypass

authentication and execute API calls on an affected device.

The vulnerability is due to insufficient access control validation. An attacker could exploit this vulnerability by sending a request to the REST API endpoint. A successful exploit could allow the attacker to interact with the REST API and cause a potential Denial of Service (DoS) condition on the affected device.

Bug ID(s): CSCvs53493, CSCvt39575
CVE ID: CVE-2020-3250
Security Impact Rating (SIR): High
CVSS Base Score: 8.6
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Cisco UCS Director and UCS Director Express for Big Data Directory Traversal Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit could allow the attacker to execute code on the system.

Bug ID(s): CSCvs69171, CSCvt39489
CVE ID: CVE-2020-3251
Security Impact Rating (SIR): High
CVSS Base Score: 8.1
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Cisco UCS Director and UCS Director Express for Big Data Directory Traversal Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit could allow the attacker to perform a Denial of Service (DoS) attack on the affected device.

Bug ID(s): CSCvs56401, CSCvt39526
CVE ID: CVE-2020-3249
Security Impact Rating (SIR): High
CVSS Base Score: 8.1
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Cisco UCS Director and UCS Director Express for Big Data Directory Traversal Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit could allow the attacker to execute code with *root* privileges.

Bug ID(s): CSCvs56400, CSCvt39535
CVE ID: CVE-2020-3248
Security Impact Rating (SIR): High
CVSS Base Score: 8.1
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Cisco UCS Director and UCS Director Express for Big Data Directory Traversal Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a malicious file to the REST API. A successful exploit could allow the attacker to write or execute arbitrary files on the system.

Bug ID(s): CSCvs53502, CSCvt39565
CVE ID: CVE-2020-3247
Security Impact Rating (SIR): High
CVSS Base Score: 8.1
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Cisco UCS Director and UCS Director Express for Big Data Directory

Traversal Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a malicious zip file to the REST API. A successful exploit could allow the attacker to write or execute arbitrary files on the system with full administrative privileges.

Bug ID(s): CSCvs53500, CSCvt39561
CVE ID: CVE-2020-3239
Security Impact Rating (SIR): High
CVSS Base Score: 8.1
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Cisco UCS Director Directory Traversal Vulnerability

A vulnerability in the REST API endpoint of Cisco UCS Director could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit could allow the attacker to read arbitrary files on the system.

Bug ID(s): CSCvs69022
CVE ID: CVE-2020-3252
Security Impact Rating (SIR): Medium
CVSS Base Score: 6.5
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

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 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.

Fixed Releases

Cisco fixed this vulnerability in UCS Director Release 6.7.4.0 and UCS Director Express for Big Data Release 3.7.4.0.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is aware that proof-of-concept exploit code is available for the vulnerabilities that are described in this advisory.

Source

Cisco would like to thank Steven Seeley (mr_me) of Source Incite working with Trend Micro Zero Day Initiative for reporting the following vulnerabilities:

- CVE-2020-3243
- CVE-2020-3240
- CVE-2020-3250
- CVE-2020-3239
- CVE-2020-3247
- CVE-2020-3248
- CVE-2020-3249

Cisco would like to thank Steven Seeley (mr_me) of Source Incite for reporting the following vulnerabilities:

- CVE-2020-3251
- CVE-2020-3252

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsd-mult-vulns-UNfpdW4E

Revision History

Version	Description	Section	Status	Date
1.1	Updated information about the availability of exploit code.	Exploitation and Public Announcements	Final	2020-APR-17
1.0	Initial public release.	-	Final	2020-APR-15