Cisco Security Advisory

Cisco Integrated Management Controller Multiple Remote Code Execution Vulnerabilities

Critical

Advisory ID: cisco-sa-ucs-api-rce-UXwpeDHd

First Published: 2020 November 18 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs: CSCvu21215 CSCvu21222 CSCvu22429 More...

CVSS Score: Base 9.8

CVE-2020-3470

Download CSAF Download CVRF Email

Summary

Multiple vulnerabilities in the API subsystem of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to execute arbitrary code with *root* privileges.

The vulnerabilities are due to improper boundary checks for certain user-supplied input. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the API subsystem of an affected system. When this request is processed, an exploitable buffer overflow condition may occur. A successful exploit could allow the attacker to execute arbitrary code with *root* privileges on the underlying operating system (OS).

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-ucs-api-rce-UXwpeDHd

Affected Products

Vulnerable Products

These vulnerabilities affect the following Cisco products if they are running a vulnerable release of Cisco IMC:

- 5000 Series Enterprise Network Compute System (ENCS) Platforms
- UCS C-Series Rack Servers in standalone mode
- UCS E-Series Servers
- UCS S-Series Servers in standalone mode

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.

Cisco has confirmed that these vulnerabilities do not affect Cisco UCS B-Series Servers, or Cisco FI-Attached C-Series and S-Series Servers managed by Cisco UCS Manager.

Workarounds

There are no workarounds to address this vulnerability.

However, administrators can disable the Cisco IMC web-management interface to mitigate the impact of these vulnerabilities. For example, the following commands show how to perform the configuration change on a UCS C-Series Server:

```
xxxxxx-bmc# scope http
xxxxxx-bmc /http #
xxxxxx-bmc /http # set enabled no
SSH is in enabled state. Disabling HTTP service
Warning: setting "enabled" to "no" will disconnect all
 existing http connections and will disable login via
WebUI.
```

```
xxxxxx-bmc /http *# commit
xxxxxx-bmc /http # show detail
HTTP Settings:
    HTTP Port: 80
    HTTPS Port: 443
    Timeout: 1800
    Max Sessions: 4
    Active Sessions: 0
    Enabled: no
    HTTP Redirected: yes
xxxxxx-bmc /http # exit
```

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.

Fixed Releases

Customers are advised to upgrade to an appropriate release as indicated in the following tables:

Cisco UCS C-Series Rack Servers

M3 Servers	Affected Firmware Release	First Fixed Firmware Release
3.0	3.0(1c) to 3.0(4q)	3.0(4r)
M4 Servers	**Affected Firmware Release**	**First Fixed Firmware Release**
3.0	3.0(1c) to 3.0(4q)	3.0(4r)
4.0	4.0(1a) to 4.0(2l)	4.0(2n)
4.1	4.1(1c) to 4.1(1f)	4.1(1g)
M5 Servers	**Affected Firmware Release**	**First Fixed Firmware Release**
3.1	All releases	Migrate to a fixed release.
4.0	4.0(1a) to 4.0(4l)	4.0(4m)
4.1	4.1(1c) to 4.1(1f)	4.1(1g)

Cisco UCS E-Series

Cisco fixed these vulnerabilities in Cisco IMC for E-Series Servers releases 3.2.11.3 and later.

Cisco UCS S-Series

Server - S3160	Affected Firmware Release	First Fixed Firmware Release
3.0	3.0(1c) to 3.0(4q)	3.0(4r)
Server - S3260	**Affected Firmware Release**	**First Fixed Firmware Release**
3.1	All releases	Migrate to a fixed release.
4.0	4.0(1a) to 4.0(4l)	4.0(4m)
4.1	4.1(1c) to 4.1(1f)	4.1(1g)

Cisco 5000 Series ENCS Platforms

Cisco fixed these vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) for Cisco 5000 Series ENCS Platforms releases 4.4.1 and later.

Exploitation and Public Announcements

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

Source

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

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-api-rce-UXwpeDHd

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2020-NOV-18