



Cisco Integrated Management Controller Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data Command Injection Vulnerability



Advisory ID:	cisco-sa-20190821-imcs-ucs-cmdinj
First Published:	2019 August 21 16:00 GMT
Last Updated:	2019 August 30 12:33 GMT CVE-2019-1936
Version 1.1:	Final
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCvp19245
CVSS Score:	Base 7.2

[Download CSAF](#) [Download CVRF](#) [Email](#)

Summary

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an authenticated, remote attacker to execute arbitrary commands on the underlying Linux shell as the *root* user. Exploitation of this vulnerability requires privileged access to an affected device.

The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by logging in to the web-based management interface with administrator privileges and then sending a malicious request to a certain part of the interface.

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

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 50903](#)

Related to This Advisory

Your Rating:

Average Rating:

5 star

workarounds that address this vulnerability.

This advisory is available at the following link:
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-cmdinj>

Affected Products

Vulnerable Products

This vulnerability affects the following Cisco products:

Cisco IMC Supervisor releases:

- 2.1
- 2.2.0.0 through 2.2.0.6

Cisco UCS Director releases:

- 6.0
- 6.5
- 6.6.0.0 and 6.6.1.0
- 6.7.0.0 and 6.7.1.0

Cisco UCS Director Express for Big Data releases:

- 3.0
- 3.5
- 3.6
- 3.7.0.0 and 3.7.1.0

Products Confirmed Not Vulnerable

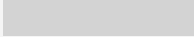
Only products listed in the [Vulnerable Products](#) section of this advisory are known to be affected by this vulnerability.

Workarounds

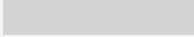
There are no workarounds that address this vulnerability.

Fixed Software

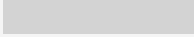
4 star



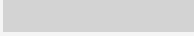
3 star



2 star



1 star



[Leave additional feedback](#)

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

Cisco fixed this vulnerability in the following software releases:

- Cisco IMC Supervisor releases 2.2.1.0 and later
- Cisco UCS Director releases 6.7.2.0 and later (recommended: 6.7.3.0)
- Cisco UCS Director Express for Big Data releases 3.7.2.0 and later (recommended: 3.7.3.0)

Customers can download the Cisco IMC Supervisor software from the [Software Center](#) on Cisco.com by doing the following:

1. Click **Browse all**.
2. Choose **Servers - Unified Computing > Integrated Management Controller (IMC) Supervisor > IMC Supervisor 2.x**.
3. Access releases by using the left pane of the **IMC Supervisor 2.x** page.

Customers can download the Cisco UCS Director software from the [Software Center](#) on Cisco.com by doing the following:

1. Click **Browse all**.
2. Choose **Servers - Unified Computing > UCS Director > UCS Director 6.7**.
3. Access releases by using the left pane of the **UCS Director 6.7** page.

Customers can download the Cisco UCS Director Express for Big Data software from the [Software Center](#) on Cisco.com by doing the following:

1. Click **Browse all**.
2. Choose **Servers - Unified Computing > UCS Director > UCS Director Express for Big Data 3.7**.
3. Access releases by using the left pane of the **UCS Director Express for Big Data 3.7** page.

Exploitation and Public Announcements

Security researcher Pedro Ribeiro has published details on this vulnerability in his GitHub repository and has also released corresponding Metasploit modules.

Source

Cisco would like to thank independent security researcher Pedro Ribeiro for reporting this vulnerability to iDefense's Vulnerability Contributor Program.

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-cmdinj>

Revision History

Version	Description	Section	Status	Date
1.1	Updated the public announcement and availability of public exploit code.	Exploitation and Public Announcements	Final	2019-August-30
1.0	Initial public release.	-	Final	2019-August-21

LEGAL DISCLAIMER

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.