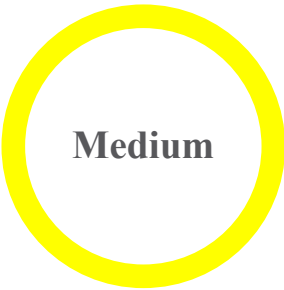




# Cisco UCS Director Information Disclosure Vulnerability



Advisory ID:	cisco-sa-20200108-ucs-dir-infodis
First Published:	2020 January 8 16:00 GMT
Version 1.0:	Final CVE-2019-16003
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCvr00602
CVSS Score:	Base 4.3

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

## Summary

A vulnerability in the web-based management interface of Cisco UCS Director could allow an unauthenticated, remote attacker to download system log files from an affected device.

The vulnerability is due to an issue in the authentication logic of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web interface. A successful exploit could allow the attacker to download log files if they were previously generated by an administrator.

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-20200108-ucs-dir-infodis>

## Affected Products

### Vulnerable Products

### 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](#)

### Related to This Advisory

#### Your Rating:

☐ ☐ ☐ ☐ ☐

#### Average Rating:

☐ ☐ ☐ ☐ ☐

5 star

4 star

3 star

2 star

At the time of publication, this vulnerability affected Cisco UCS Director releases earlier than Release 6.7.3.1.

See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

## 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

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.

## Fixed Releases

At the time of publication, Cisco UCS Director releases 6.7.3.1 and later contained the fix for this vulnerability.

See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

## 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

1 star

[Leave additional feedback](#)

advisory.

## Source

This vulnerability was found during internal security testing.

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200108-ucs-dir-infodis>

## Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2020-January-08

### 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.