Cisco Security Advisory

Cisco UCS Director Information Disclosure Vulnerability

Medium

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

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

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