Cisco Security Advisory

Cisco Unified Computing System BIOS Signature Bypass Vulnerability

Medium

Advisory ID:	cisco-sa-20190605-ucs-biossig-bypass		Email
First Published:	2019 June 5 16:00 GMT	CVE-2019-1880	
Last Updated:	2019 August 1 13:20 GMT		
Version 1.1:	Final		
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvp12824 CSCvp12840		
CVSS Score: Base 4.4			

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

Your Rating:

□ □ □ □ □

Average Rating:

□ □ □ □ □

5 star

0

4 star

0

3 star

0

2 star

0

Summary

A vulnerability in the BIOS upgrade utility of Cisco Unified Computing System (UCS) C-Series Rack Servers could allow an authenticated, local attacker to install compromised BIOS firmware on an affected device.

The vulnerability is due to insufficient validation of the firmware image file. An attacker could exploit this vulnerability by executing the BIOS upgrade utility with a specific set of options. A successful exploit could allow the attacker to bypass the firmware signature-verification process and install compromised BIOS firmware on an affected device.

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-20190605-ucs-biossig-bypass

1 star

0

Leave additional feedback

Affected Products

Vulnerable Products

This vulnerability affects the following Cisco products:

- UCS C125 M5 Rack Server Node
- UCS C220 M4 Rack Server
- UCS C220 M5 Rack Server
- UCS C240 M4 Rack Server
- UCS C240 M5 Rack Server
- UCS C460 M4 Rack Server
- UCS C480 M5 Rack Server
- Cisco Secure Network Server 3415
- Cisco Secure Network Server 3495
- Cisco Secure Network Server 3515
- Cisco Secure Network Server 3595

For information about affected software releases, consult the Cisco bug ID(s) at the top of this advisory.

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

For information about fixed software releases, consult the Cisco bug ID(s) at the top of this advisory.

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.

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-20190605-ucs-biossig-bypass

Revision History

Version	Description	Section	Status	Date
1.1	Added Cisco Secure Network Server models	Affected products	Final	2019-August-01
1.0	Initial public release.	-	Final	2019-June-05

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.