Cisco Security Advisory

Vulnerabilities in OpenSSL Affecting Cisco Products: November 2022

High

Advisory ID:
cisco-sa-openssl-W9sdCc2a

First Published:
2022 October 28 16:00 GMT

Last Updated:
2022 November 23 20:23 GMT

Version 1.6: Final

Workarounds: No workarounds available

CVE-2022-3602

CVE-2022-3786

CVSS Score:
Base 7.5

Download CSAF

Email

Summary

On November 1, 2022, the OpenSSL Project announced the following vulnerabilities:

CVE-2022-3602 - X.509 Email Address 4-byte Buffer Overflow
CVE-2022-3786 - X.509 Email Address Variable Length Buffer Overflow

For a description of these vulnerabilities, see OpenSSL Security Advisory [Nov 1 2022].

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssl-W9sdCc2a

Affected Products

Cisco investigated its product line to determine which products and cloud services may be affected by these vulnerabilities. OpenSSL 3.x is not widely used in Cisco products and cloud offers, and only products that may contain the affected software are listed in this advisory. If a product or cloud offer is not explicitly listed in this advisory, it is not vulnerable.

Vulnerable Products

The following table lists Cisco products that are affected by one or more of the vulnerabilities that are described in this advisory. If a future release date is indicated for software, the date provided represents an estimate based on all information known to Cisco as of the Last Updated date at the top of the advisory. Availability dates are subject to change based on a number of factors, including satisfactory testing results and delivery of other priority features and fixes. If no version or date is listed for an affected component (indicated by a blank field and/or an advisory designation of Interim), Cisco is continuing to evaluate the fix and will update the advisory as additional information becomes available. After the advisory is marked Final, customers should refer to the associated Cisco bug(s) for further details.

Product	Cisco Bug ID	Fixed Release Availability
Endpoint Clients and Client Software		
Operational Insights Collector	CSCwd44110	ScienceLogic Application Software 3.0.1 (Nov 2022) HPNA Application Software 2.0.1 (Nov 2022) APIC Application Software 3.0.1 (Nov 2022) SolarWinds Application Software 3.0.1 (Nov 2022) Syslog Collector 2.0.1 (Nov 2022)
Network Management and Provisioning		
IoT Field Network Director, formerly Connected Grid Network Management System	CSCwd44112	4.8.1 (Available) 4.9.0 (Available) 5.0.0 (May 2023)

Products Confirmed Not Vulnerable

Only products that may contain the affected software are listed in this advisory. If a product or cloud offer is not explicitly listed in this advisory, it is not vulnerable.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

Network and Content Security Devices

- Identity Services Engine (ISE)

- Secure Network Analytics, formerly Stealthwatch

Network Management and Provisioning

- Application Policy Infrastructure Controller (APIC)
- Cisco Container Platform
- Data Center Network Manager (DCNM)
- Elastic Services Controller (ESC)
- Evolved Programmable Network Manager
- Nexus Dashboard, formerly Application Services Engine
- Prime Infrastructure

Routing and Switching - Enterprise and Service Provider

- SD-WAN vAnalytics
- SD-WAN vManage
- Ultra Cloud Core - Network Respository Function
- Ultra Cloud Core - Policy Control Function
- Ultra Cloud Core - Redundancy Configuration Manager
- Ultra Cloud Core - Subscriber Microservices Infrastructure
- Ultra Cloud Core - User Plane Function

Unified Computing

- HyperFlex System
- UCS Blade Server - Integrated Management Controller
- UCS Manager

Cisco Cloud Offerings

Cisco investigated its cloud offers to determine which products may be affected by these vulnerabilities. The following table lists Cisco cloud offers that are under investigation. Only cloud offers known to possibly be affected are listed. If a cloud offer is not explicitly listed in this advisory, it is not vulnerable.

Product	Disposition
AppDynamics	Not affected
CX Cloud	Not affected
Duo	Not affected
Intersight	Not affected
Meraki	Not affected
SD-WAN	Not affected
SecureX	Not affected
ThousandEyes	Not affected
Umbrella	Not affected
Unified Communications Manager Cloud	Not affected
Webex Calling	Not affected
Webex Cloud-Connected UC	Not affected
Webex Contact Center	Not affected
Webex Teams	Not affected

Workarounds

Any workarounds for a specific Cisco product or service will be documented in the relevant Cisco bugs, which are identified in the Vulnerable Products section of this advisory.

Fixed Software

For information about fixed software releases, consult the Cisco bugs identified in the Vulnerable Products section 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 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 malicious use of the vulnerabilities that are described in this advisory.

Source

These vulnerabilities were publicly disclosed by the OpenSSL Software Foundation on November 1, 2022.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssl-W9sdCc2a

Revision History

Version	Description	Section	Status	Date
1.6	Updated vulnerable products and products confirmed not vulnerable.	Affected Products	Final	2022-NOV-23
1.5	Update summary, affected products, and disposition of cloud offers.	Summary, Affected Products	Final	2022-NOV-08

Show Complete History...

Legal Disclaimer

- Cisco Security Vulnerability Policy
- Subscribe to Cisco Security Notifications
- Action Links for This Advisory
- Related to This Advisory