Multiple Cisco Products Unauthenticated Remote Code Execution in Erlang/OTP SSH Server:

Updated: April 30, 2025 **Document ID:** 1745360245562120

Bias-Free Langua

Cisco Security Advisory

Multiple Cisco Products Unauthenticated Remote Code Execution in Erlang/OTP SSH Server: April 2025

Advisory ID:
cisco-sa-erlang-otp-ssh-xyZZy

First Published:
2025 April 22 21:45 GMT

Last Updated:
2025 April 30 19:27 GMT

Version 1.6: Interim

Workarounds: No workarounds available

CVE-2025-32433

CWE-306

CVSS Score:
Base 10.0 **Click Icon to Copy Verbose Score**
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:X/RC:X

Download CSAF Email

Summary

On April 16, 2025, a critical vulnerability in the Erlang/OTP SSH server was disclosed. This vulnerability could allow an unauthenticated, remote attacker to perform remote code execution (RCE) on an affected device.

The vulnerability is due to a flaw in the handling of SSH messages during the authentication phase.

For a description of this vulnerability, see the Erlang announcement.

This advisory will be updated as additional information becomes available.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy

Affected Products

Cisco has investigated its product lines that include Erlang/OTP to determine which products may be affected by this vulnerability.

This advisory only lists Cisco products and services that are known to include the impacted software component and thus may be vulnerable. Products and services that do not contain the impacted software component are not vulnerable and therefore are not listed in this advisory. Any Cisco product or service that is not explicitly listed in the Affected Products section of this advisory is not affected by the vulnerability or vulnerabilities described.

The Vulnerable Products section includes Cisco bug IDs for each affected product. The bugs are accessible through the Cisco Bug Search Tool and contain additional platform-specific information, including workarounds (if

available) and fixed software releases.

Vulnerable Products

The following table lists Cisco products that are affected by the vulnerability that is 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.

Cisco Product	Cisco Bug ID	Fixed Release Available
Network Application, Service, and Acceleration		
ConfD, ConfD Basic[1]	CSCwo83759	7.7.19.1 8.0.17.1 8.1.16.2 8.2.11.1 8.3.8.1 (May 2025) 8.4.4.1 (May 2025)
Network Management and Provisioning		
Network Services Orchestrator (NSO)[1]	CSCwo83796	5.7.19.1 6.1.16.2 6.2.11.1 6.3.8.1 6.4.1.1 6.4.4.1
Smart PHY[1]	CSCwo83751	
Ultra Services Platform[1]	CSCwo83750	
Routing and Switching - Enterprise and Service Provider		
ASR 5000 Series Software (StarOS) and Ultra Packet Core[1]	CSCwo83806	
Cloud Native Broadband Network Gateway[1]	CSCwo83769	
iNode Manager	CSCwo83755	No fix planned.[2]
Optical Site Manager for Network Convergence System (NCS) 1000 Series[1]	CSCwo83800	25.2.1 (Jun 2025) 25.3.1 (Sep 2025)
Shelf Virtualization Orchestrator Module for NCS 2000 Series[1]	CSCwo83774	
Ultra Cloud Core - Access and Mobility Management Function[1]	CSCwo83785	
Ultra Cloud Core - Policy Control Function[1]	CSCwo83789	
Ultra Cloud Core - Redundancy Configuration Manager[1]	CSCwo83753	
Ultra Cloud Core - Session Management Function[1]	CSCwo83775	
Ultra Cloud Core - Subscriber Microservices Infrastructure[1]	CSCwo83747	2025.03.1 (Aug 2025)
Unified Computing		
Enterprise NFV Infrastructure Software (NFVIS)[1]	CSCwo83758	
Routing and Switching - Small Business		
Small Business RV Series Routers RV160, RV160W, RV260, RV260P, RV260W, RV340, RV340W, RV345, RV345P	CSCwo83803 CSCwo83767	No fix planned.[3]

1. While these products are vulnerable because they accept unauthenticated channel request messages, due to the product configuration they are not vulnerable to RCE.
2. iNode Manager has reached end of software maintenance. End-of-Sale and End-of-Life Announcement for the Cisco iNode Manager & Intelligent Node Local Control Software.
3. These routers have reached end of software maintenance. End-of-Sale and End-of-Life Announcement for the Cisco RV 160, RV260, RV345P, RV340W, RV260W, RV260P and RV160W VPN Routers.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

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

Network and Content Security Devices
FXOS Software
Identity Services Engine (ISE)
Secure Adaptive Security Appliance (ASA) Software
Secure Firewall Management Center (FMC) Software
Secure Firewall Threat Defense (FTD) Software
Secure Network Analytics (SNA)
Network Application, Service, and Acceleration
Automated Fault Management
Wide Area Application Services (WAAS) Software
Network Management and Provisioning
Application Policy Infrastructure Controller (APIC)
Crosswork Hierarchical Controller
Cyber Vision
Elastic Services Controller
Evolved Programmable Network Manager (EPNM)
FindIT Network Management Software
Policy Suite
Provider Connectivity Assurance
Virtual Topology System
Virtualized Infrastructure Manager
WAE Automation
Routing and Switching - Enterprise and Service Provider
Catalyst Center
Catalyst SD-WAN Manager
Catalyst SD-WAN
Intelligent Node Software
IOS Software
IOS XE Software
IOS XR Software
Meraki Products
NX-OS Software
Routing and Switching - Small Business
Business Dashboard
Video, Streaming, TelePresence, and Transcoding Devices
Expressway and TelePresence Video Communication Server (VCS)

Workarounds

Any workarounds will be documented in the product-specific 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 aware that proof-of-concept exploit code is available for the vulnerability described in this advisory.

The Cisco PSIRT is not aware of any malicious use of the vulnerability that is described in this advisory.

Source

This vulnerability was reported publicly through the Erlang/OTP Github Issues Tracker.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy

Revision History

Version	Description	Section	Status	Date
1.6	Updated product lists and statuses.	Vulnerable Products	Interim	2025-APR-30
1.5	Updated product lists and statuses.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2025-APR-29

Show Complete History...

Legal Disclaimer

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory

Quick Links

About Cisco

Contact Us

Careers

Connect with a partner

Resources and Legal

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap