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

April 2025

SOC Informative Report

Document details

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

Summary
Report containing information about a vulnerability detected in the product Erlang/OTP SSH, categorized as *Unauthenticated Remote Code Execution.*

Target audience
SOC and SOC AdS representatives

Confidentiality level (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Publication date
28/04/2025

Written by
Matteo Lorenzini

Reviewed by
Massimo Giaimo

Confidentiality level

A level of confidentiality is applied to the document, marked by the "Confidentiality Level" item on the front page. The values that can be used (RED / AMBER / AMBER+STRICT / GREEN / CLEAR) have the following meanings:

TLP:RED = Reserved for participants only.

> Sources may use TLP:RED when the information cannot be effectively used by other parties and could impact a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with parties outside the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most cases, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

TLP:AMBER+STRICT limits sharing to the *organization* only.

> Sources may use TLP:AMBER when the information requires support to act effectively but poses risks to privacy, reputation, or operations if shared outside the organizations involved. Recipients may share TLP:AMBER information only with members of their own organization and with clients or customers who need to know the information to protect themselves or prevent further harm.
>
> Note: If the source wishes to limit sharing **only** to the organization, it must specify TLP:AMBER+STRICT.

TLP:GREEN =Limited disclosure, restricted to the community.

> Sources may use TLP:GREEN when the information is useful for the awareness of all participating organizations, as well as with colleagues within the community or broader sector. Recipients may share TLP:GREEN information with colleagues and partner organizations within their sector or community, but not through publicly accessible channels. Information in this category may be widely disseminated within a particular community. TLP:GREEN information may not be released outside the community.

TLP:CLEAR = Disclosure is not limited.

Sources may use TLP:CLEAR when the information poses little or foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

Table of contents

Introduction

Erlang/OTP SSH is a set of libraries that allows developers to embed SSH server or client functionality directly into Erlang applications. Erlang/OTP is commonly found in IoT devices and telecommunications platforms/systems.

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.

As of the time of writing (28/04/2025), multiple exploits and proof-of-concept (PoC) codes for these vulnerabilities are publicly available[1]. Cisco PSIRT is not aware of any malicious use of the vulnerability described in this advisory.

A new Metasploit module for this vulnerability is now available for testing and validation purposes[2].

The following is a table containing the details of the vulnerability:

CVE Number	CVSS Score	EPSS Score
CVE-2025-32433[3]	10.0 (Critical)	3.9% (Low)

Overview of the CVE

CVE-2025-32433

This is a critical vulnerability in the Erlang/OTP SSH implementation that allows unauthenticated remote code execution. The flaw exists in the handling of SSH protocol messages, where an attacker can send connection protocol messages before authentication occurs. This bypass enables the execution of arbitrary code on the target system without prior authentication.

The vulnerability affects any system running an SSH server based on the Erlang/OTP SSH library and is classified with a CVSS v3.1 score of 10.0, indicating maximum severity. Successful exploitation may lead to full system compromise, including unauthorized access, data manipulation, and denial of service, especially if the SSH daemon runs with elevated privileges.

Remediation

Cisco is investigating its product lines which include Erlang/OTP to determine which products may be affected by this vulnerability. As the investigation progresses, Cisco will update this advisory with information about affected products on its site[4].

Vulnerable Products

Category	Cisco Product	Cisco Bug ID[5]	Fixed Release Available
Network Application, Service, and Acceleration	ConfD, ConfD Basic[6]	CSCwo83759	7.7.19.1 (May 2025) 8.1.16.2 (May 2025) 8.4.4.1 (May 2025)
Network Management and Provisioning	Network Services Orchestrator (NSO)[6]	CSCwo83796	5.7.19.1 (May 2025) 6.1.16.2 (May 2025) 6.4.1.1 6.4.4.1 (May 2025)

	Smart PHY[6]	CSCwo83751	
	Ultra Services Platform[6]	CSCwo83750	
Routing & Switching – Enterprise and Service Provider	ASR 5000 Series Software (StarOS) and Ultra Packet Core[6]	CSCwo83806	
	Cloud Native Broadband Network Gateway[6]	CSCwo83769	
	iNode Manager	CSCwo83755	No fix planned. [7]
	Ultra Cloud Core - Access and Mobility Management Function[6]	CSCwo83785	
	Ultra Cloud Core - Policy Control Function[6]	CSCwo83789	
	Ultra Cloud Core - Redundancy Configuration Manager[6]	CSCwo83753	
	Ultra Cloud Core - Session Management Function[6]	CSCwo83775	
	Ultra Cloud Core - Subscriber Microservices Infrastructure[6]	CSCwo83747	

Unified Computing	Enterprise NFV Infrastructure Software (NFVIS)[6]	CSCwo83758	
Routing & Switching – Small Business	Small Business RV Series Routers RV160, RV160W, RV260, RV260P, RV260W, RV340, RV340W, RV345, RV345P	CSCwo83803 CSCwo83767	No fix planned. [8]

Erlang/OTP SSH fixies are available, users are advised to update to OTP-27.3.3 (for OTP-27), OTP-26.2.5.11 (for OTP-26), or OTP-25.3.2.20 (for OTP-25) to mitigate this issue. [9]

Until upgrading to a fixed version, we recommend disabling the SSH server or to prevent access via firewall rules.

Attack surface

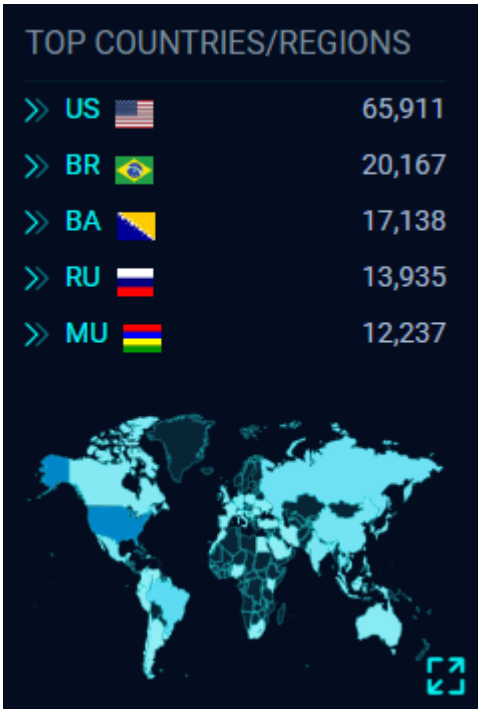
A quick search on Shodan returns 92k exposed instances of SSH-2.0-Cisco-1.25 that may be vulnerable if not patched. Most of them are located in the US. Below are the devices found with the Shodan query (SSH-2.0-Cisco-1.25, search date 24/04/2025):

Shodan Query
SSH-2.0-Cisco-1.25

While doing the same research on Censys the number has increased up to 103k.

Censys Query
services.ssh.endpoint_id.raw="SSH-2.0-Cisco-1.25"


While doing the same research on FOFA the number has increased up to 309k.

FOFA query
SSH-2.0-Cisco-1.25


Bibliography

[1] https://github.com/omer-efe-curkus/CVE-2025-32433-Erlang-OTP-SSH-RCE-PoC

[2] https://github.com/rapid7/metasploit-framework/pull/20060#pullrequestreview-2781805383

[3] https://nvd.nist.gov/vuln/detail/CVE-2025-32433

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

[5] https://tools.cisco.com/bugsearch/bug/{BugID}

[6] While these products are vulnerable because they accept unauthenticated channel request messages, due to the product configuration they are not vulnerable to RCE.

[7] 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.

[8] 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.

[9] https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2