Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability

Vulnerability Note: VN-2025-28

Date of Issue: 02 October 2025

Severity Rating: High

Systems Affected:

This vulnerability affects Cisco devices if they are running a vulnerable release of Cisco IOS and IOS XE Software and if they are configured to use TACACS+ but are missing the TACACS+ shared secret.

Description

A vulnerability in the implementation of the TACACS+ protocol in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to view sensitive data or bypass authentication.

This vulnerability exists because the system does not properly check whether the required TACACS+ shared secret is configured. A machine-in-the-middle attacker could exploit this vulnerability by intercepting and reading unencrypted TACACS+ messages or impersonating the TACACS+ server and falsely accepting arbitrary authentication requests. A successful exploit could allow the attacker to view sensitive information in a TACACS+ message or bypass authentication and gain access to the affected device.

CVE Information
[CVE-2025-20160](CVE-2025-20160)

Workaround
Cisco has released free software updates that address the vulnerability described in this advisory.
Users are recommended to apply the updates.
More information is available on:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-tacacs-hdB7thJw

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,

Cybercity Ebene