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

CERT-MU Vulnerability Note

Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability

Vulnerability Note: VN-2025-19

Date of Issue: 20 August 2025

Severity Rating: High

Systems Affected:

- This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS or IOS XE Software and have the Smart Install client feature enabled.

Description

A vulnerability has been identified in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software. The vulnerability could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device.

The vulnerability is caused due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device, which could have the following impacts:

- Triggering a reload of the device
- Allowing the attacker to execute arbitrary code on the device
- Causing an indefinite loop on the affected device that triggers a watchdog crash

CVE Information
CVE-2018-0171

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-20180328-smi2

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