

CVE-2018-0171

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

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software 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 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.

EVRS

87/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.995

99.94th percentile · FIRST

CISA DEADLINE

May 3, 2022

KEV since 2021 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.995 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

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. Cisco Bug IDs: CSCvg76186.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	15.2(5)e	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4w6g-87mh-x63x**NVD** nvd.nist.gov/vuln/detail/CVE-2018-0171**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2018-0994**Additional guidance** tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog**Current data** evulnable.com/vulnerability-management/cve/CVE-2018-0171

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.