CVE-2017-6739

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-6739
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-17 21:29:00 UTC
Updated	2026-04-22 15:51:27 UTC
Description	A vulnerability in the SNMP implementation of could allow an authenticated, remote attacker to cause a reload of the affecte

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.203550000 probability, percentile 0.955490000 (date 2026-04-25)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

Problem Types: CWE-119 | CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.0	psirt@cisco.com	Secondary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.0	CNA	CVSSV3_0	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

AV:N/AC:L/Au:S/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	IOS and IOS XE Software
Name	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-6739

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	All	All	All	All
Operating System	Cisco	Ios	All	All	All	All
Operating System	Cisco	Ios Xe	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	IntelliShield	Universal Product	affected N/A	Not specified

References

Reference	Source
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-
Cisco IOS/IOS XE Buffer Overflow in SNMP Service Lets Remote Authenticated Users Execute Arbitrary Code - SecurityTracker	af854a3a-
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-201706...	psirt@cisc
Cisco IOS and IOS XE Software Multiple Remote Code Execution Vulnerabilities	af854a3a-
SNMP Remote Code Execution Vulnerabilities in Cisco IOS and IOS XE Software	af854a3a-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-03T00:00:00.000Z	CVE-2017-6739 added to CISA KEV

Exploits

CNA: At the time of initial publication, Cisco was aware of external knowledge of the vulnerabilities described in this advisory and, as a precaution, notified customers about the potential for exploitation. On January 6, 2017, a security researcher published functional exploit code for these vulnerabilities. The Cisco Product Security Incident Response Team (PSIRT) is aware of exploitation of the following vulnerabilities that are described in this advisory: CVE-2017-6736 CVE-2017-6737 CVE-2017-6738 CVE-2017-6739 CVE-2017-6740 CVE-2017-6742 CVE-2017-6743 CVE-2017-6744 The Cisco PSIRT is aware of exploit code available for CVE-2017-6741. Additional information can be found at Cisco TALOS: DNS Hijacking Abuses Trust In Core Internet Service ["https://blog.talosintelligence.com/2019/04/seaturtle.html"].

Legacy QID Mappings

590342 Rockwell Automation Allen-Bradley Stratix and ArmorStratix Multiple Vulnerabilities (ICSA-17-208-04)