



# CVE-2017-6742

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-6742
<b>State</b>	PUBLISHED
<b>Assigner</b>	cisco
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-07-17 21:29:00 UTC
<b>Updated</b>	2026-04-22 14:51:43 UTC
<b>Description</b>	A vulnerability in the SNMP implementation of could allow an authenticated, remote attacker to cause a reload of the affect

## 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:** 0.120600000 probability, percentile 0.938200000 (date 2026-04-25)

**CISA KEV:** Listed on 2023-04-19; due 2023-05-10; ransomware use Unknown

**Problem Types:** CWE-119 | 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



CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	IOS and IOS XE Software
<b>Name</b>	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmpp">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmpp</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2017-6742">https://nvd.nist.gov/vuln/detail/CVE-2017-6742</a>

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	Cisco	Cisco IOS XE Software	affected 3.7.0S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.1S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.2S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.3S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.4S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.5S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.6S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.7S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.4aS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.2tS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.0bS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.8.0S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.8.1S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.8.2S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.9.1S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.9.0S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.9.2S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.9.0aS	Not specified



CNA	Cisco	Cisco IOS XE Software	affected 3.15.3S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.15.4S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.4E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.5E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.0S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.1S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.1aS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.2S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.0cS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.3S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.2bS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.4aS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.4bS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.5S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.16.4dS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.17.0S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.17.1S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.17.2S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.17.1aS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.17.3S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.2.1	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.2.2	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.3.1	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.3.2	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.3.3	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.3.1a	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.3.4	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.4.1	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.4.2	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.5.1	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.5.1b	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.18.0aS	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.18.0S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.18.1S	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.18.0SP	Not specified

CNA	Cisco	Cisco IOS XE Software	affected 3.18.1SP	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.18.1aSP	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.18.2aSP	Not specified
CNA	IntelliShield	Universal Product	affected N/A	Not specified

## References

Reference	Source
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
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-
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

### 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)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)