CVE-2017-6738

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

Summary

CVE	CVE-2017-6738
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 15:48:04 UTC
Description	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS and IOS XE Software contains multiple vulner

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-2017-6738

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	IOS	affected 12.2(53)SE1	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE	Not specified
CNA	Cisco	IOS	affected 12.2(50)SE2	Not specified
CNA	Cisco	IOS	affected 12.2(50)SE1	Not specified
CNA	Cisco	IOS	affected 12.2(50)SE5	Not specified
CNA	Cisco	IOS	affected 12.2(53)SE	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE3	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE2	Not specified
CNA	Cisco	IOS	affected 12.2(52)SE	Not specified
CNA	Cisco	IOS	affected 12.2(58)SE	Not specified
CNA	Cisco	IOS	affected 12.2(50)SE3	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE1	Not specified
CNA	Cisco	IOS	affected 12.2(53)SE2	Not specified
CNA	Cisco	IOS	affected 12.2(52)SE1	Not specified
CNA	Cisco	IOS	affected 12.2(54)SE	Not specified
CNA	Cisco	IOS	affected 12.2(50)SE4	Not specified
CNA	Cisco	IOS	affected 12.2(50)SE	Not specified
CNA	Cisco	IOS	affected 12.2(58)SE1	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE4	Not specified

CNA	Cisco	IOS	affected 12.2(58)SE2	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE5	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE6	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE7	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE8	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE9	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE10	Not specified
CNA	Cisco	IOS	affected 12.2(55)SE11	Not specified
CNA	Cisco	IOS	affected 12.2(53)EX	Not specified
CNA	Cisco	IOS	affected 12.2(52)EX	Not specified
CNA	Cisco	IOS	affected 12.2(55)EX	Not specified
CNA	Cisco	IOS	affected 12.2(52)EX1	Not specified
CNA	Cisco	IOS	affected 12.2(55)EX1	Not specified
CNA	Cisco	IOS	affected 12.2(55)EX2	Not specified
CNA	Cisco	IOS	affected 12.2(55)EX3	Not specified
CNA	Cisco	IOS	affected 12.2(58)EX	Not specified
CNA	Cisco	IOS	affected 12.2(55)EY	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY1	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY	Not specified
CNA	Cisco	IOS	affected 12.2(53)EY	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY2	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY1b	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY1c	Not specified
CNA	Cisco	IOS	affected 12.2(58)EY	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY3	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY2a	Not specified
CNA	Cisco	IOS	affected 12.2(58)EY1	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY4	Not specified
CNA	Cisco	IOS	affected 12.2(52)EY3a	Not specified
CNA	Cisco	IOS	affected 12.2(58)EY2	Not specified
CNA	Cisco	IOS	affected 12.2(58)EZ	Not specified
CNA	Cisco	IOS	affected 12.2(53)EZ	Not specified
CNA	Cisco	IOS	affected 12.2(55)EZ	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ1	Not specified

CNA	Cisco	IOS	affected 12.2(60)EZ2	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ3	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ4	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ5	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ6	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ7	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ8	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ9	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ10	Not specified
CNA	Cisco	IOS	affected 12.2(60)EZ11	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG3	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG6	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG1	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG2	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG5	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG3	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG8	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG2	Not specified
CNA	Cisco	IOS	affected 12.2(54)SG1	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG1	Not specified
CNA	Cisco	IOS	affected 12.2(52)SG	Not specified
CNA	Cisco	IOS	affected 12.2(54)SG	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG7	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG4	Not specified
CNA	Cisco	IOS	affected 12.2(50)SG4	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG5	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG6	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG7	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG8	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG9	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG10	Not specified
CNA	Cisco	IOS	affected 12.2(53)SG11	Not specified
CNA	Cisco	IOS	affected 12.2(33)SXI	Not specified
CNA	Cisco	IOS	affected 12.2(33)SXI1	Not specified

CNA	Cisco	IOS	affected 12.2(52)XO	Not specified
CNA	Cisco	IOS	affected 12.2(54)XO	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ2	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ1	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ3	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ4	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ5	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ6	Not specified
CNA	Cisco	IOS	affected 12.2(50)SQ7	Not specified
CNA	Cisco	IOS	affected 15.0(1)XO1	Not specified
CNA	Cisco	IOS	affected 15.0(1)XO	Not specified
CNA	Cisco	IOS	affected 15.0(2)XO	Not specified
CNA	Cisco	IOS	affected 15.3(1)T	Not specified
CNA	Cisco	IOS	affected 15.3(2)T	Not specified
CNA	Cisco	IOS	affected 15.3(1)T1	Not specified
CNA	Cisco	IOS	affected 15.3(1)T2	Not specified
CNA	Cisco	IOS	affected 15.3(1)T3	Not specified
CNA	Cisco	IOS	affected 15.3(1)T4	Not specified
CNA	Cisco	IOS	affected 15.3(2)T1	Not specified
CNA	Cisco	IOS	affected 15.3(2)T2	Not specified
CNA	Cisco	IOS	affected 15.3(2)T3	Not specified
CNA	Cisco	IOS	affected 15.3(2)T4	Not specified
CNA	Cisco	IOS	affected 15.0(1)EY	Not specified
CNA	Cisco	IOS	affected 15.0(1)EY1	Not specified
CNA	Cisco	IOS	affected 15.0(1)EY2	Not specified
CNA	Cisco	IOS	affected 15.0(2)EY	Not specified
CNA	Cisco	IOS	affected 15.0(2)EY1	Not specified
CNA	Cisco	IOS	affected 15.0(2)EY2	Not specified
CNA	Cisco	IOS	affected 15.0(2)EY3	Not specified
CNA	Cisco	IOS	affected 12.2(54)WO	Not specified
CNA	Cisco	IOS	affected 15.0(1)SE	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE	Not specified
CNA	Cisco	IOS	affected 15.0(1)SE1	Not specified
CNA	Cisco	IOS	affected 15.0(1)SE2	Not specified

CNA	Cisco	IOS	affected 15.0(1)SE3	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE1	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE2	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE3	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE4	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE5	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE6	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE7	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE8	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE9	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE10	Not specified
CNA	Cisco	IOS	affected 15.0(2)SE10a	Not specified
CNA	Cisco	IOS	affected 15.1(1)SG	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG	Not specified
CNA	Cisco	IOS	affected 15.1(1)SG1	Not specified
CNA	Cisco	IOS	affected 15.1(1)SG2	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG1	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG2	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG3	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG4	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG5	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG6	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG7	Not specified
CNA	Cisco	IOS	affected 15.1(2)SG8	Not specified
CNA	Cisco	IOS	affected 15.2(4)M	Not specified
CNA	Cisco	IOS	affected 15.2(4)M1	Not specified
CNA	Cisco	IOS	affected 15.2(4)M2	Not specified
CNA	Cisco	IOS	affected 15.2(4)M4	Not specified
CNA	Cisco	IOS	affected 15.2(4)M3	Not specified
CNA	Cisco	IOS	affected 15.2(4)M5	Not specified
CNA	Cisco	IOS	affected 15.2(4)M8	Not specified
CNA	Cisco	IOS	affected 15.2(4)M10	Not specified
CNA	Cisco	IOS	affected 15.2(4)M7	Not specified
CNA	Cisco	IOS	affected 15.2(4)M6	Not specified
CNA	Cisco	IOS	affected 15.2(4)M9	Not specified

CNA	Cisco	IOS	affected 15.2(4)M6a	Not specified
CNA	Cisco	IOS	affected 15.2(4)M11	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG1	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG2	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG3	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG4	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG5	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG6	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG7	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG8	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG9	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG10	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG11	Not specified
CNA	Cisco	IOS	affected 15.0(2)SG11a	Not specified
CNA	Cisco	IOS	affected 15.0(1)EX	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX1	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX2	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX3	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX4	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX5	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX8	Not specified
CNA	Cisco	IOS	affected 15.0(2a)EX5	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX10	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX11	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX13	Not specified
CNA	Cisco	IOS	affected 15.0(2)EX12	Not specified
CNA	Cisco	IOS	affected 15.2(2)GC	Not specified
CNA	Cisco	IOS	affected 15.2(3)GC	Not specified
CNA	Cisco	IOS	affected 15.2(3)GC1	Not specified
CNA	Cisco	IOS	affected 15.2(4)GC	Not specified
CNA	Cisco	IOS	affected 15.2(4)GC2	Not specified
CNA	Cisco	IOS	affected 15.2(4)GC3	Not specified
CNA	Cisco	IOS	affected 15.4(1)T	Not specified
CNA	Cisco	IOS	affected 15.4(2)T	Not specified

CNA	Cisco	IOS	affected 15.4(1)T2	Not specified
CNA	Cisco	IOS	affected 15.4(1)T1	Not specified
CNA	Cisco	IOS	affected 15.4(1)T3	Not specified
CNA	Cisco	IOS	affected 15.4(2)T1	Not specified
CNA	Cisco	IOS	affected 15.4(2)T3	Not specified
CNA	Cisco	IOS	affected 15.4(2)T2	Not specified
CNA	Cisco	IOS	affected 15.4(1)T4	Not specified
CNA	Cisco	IOS	affected 15.4(2)T4	Not specified
CNA	Cisco	IOS	affected 15.0(2)EA	Not specified
CNA	Cisco	IOS	affected 15.0(2)EA1	Not specified
CNA	Cisco	IOS	affected 15.2(1)E	Not specified
CNA	Cisco	IOS	affected 15.2(2)E	Not specified
CNA	Cisco	IOS	affected 15.2(1)E1	Not specified
CNA	Cisco	IOS	affected 15.2(3)E	Not specified
CNA	Cisco	IOS	affected 15.2(1)E2	Not specified
CNA	Cisco	IOS	affected 15.2(1)E3	Not specified
CNA	Cisco	IOS	affected 15.2(2)E1	Not specified
CNA	Cisco	IOS	affected 15.2(4)E	Not specified
CNA	Cisco	IOS	affected 15.2(3)E1	Not specified
CNA	Cisco	IOS	affected 15.2(2)E2	Not specified
CNA	Cisco	IOS	affected 15.2(2a)E1	Not specified
CNA	Cisco	IOS	affected 15.2(2)E3	Not specified
CNA	Cisco	IOS	affected 15.2(2a)E2	Not specified
CNA	Cisco	IOS	affected 15.2(3)E2	Not specified
CNA	Cisco	IOS	affected 15.2(3a)E	Not specified
CNA	Cisco	IOS	affected 15.2(3)E3	Not specified
CNA	Cisco	IOS	affected 15.2(4)E1	Not specified
CNA	Cisco	IOS	affected 15.2(2)E4	Not specified
CNA	Cisco	IOS	affected 15.2(2)E5	Not specified
CNA	Cisco	IOS	affected 15.2(4)E2	Not specified
CNA	Cisco	IOS	affected 15.2(3)E4	Not specified
CNA	Cisco	IOS	affected 15.2(5)E	Not specified
CNA	Cisco	IOS	affected 15.2(4)E3	Not specified
CNA	Cisco	IOS	affected 15.2(2)E6	Not specified
CNA	Cisco	IOS	affected 15.2(5a)E	Not specified

CNA	Cisco	IOS	affected 15.2(5)E1	Not specified
CNA	Cisco	IOS	affected 15.2(5b)E	Not specified
CNA	Cisco	IOS	affected 15.2(2)E5a	Not specified
CNA	Cisco	IOS	affected 15.2(5c)E	Not specified
CNA	Cisco	IOS	affected 15.2(2)E5b	Not specified
CNA	Cisco	IOS	affected 15.2(5a)E1	Not specified
CNA	Cisco	IOS	affected 15.2(4)E4	Not specified
CNA	Cisco	IOS	affected 15.2(5)E2	Not specified
CNA	Cisco	IOS	affected 15.3(3)M	Not specified
CNA	Cisco	IOS	affected 15.3(3)M1	Not specified
CNA	Cisco	IOS	affected 15.3(3)M2	Not specified
CNA	Cisco	IOS	affected 15.3(3)M3	Not specified
CNA	Cisco	IOS	affected 15.3(3)M5	Not specified
CNA	Cisco	IOS	affected 15.3(3)M4	Not specified
CNA	Cisco	IOS	affected 15.3(3)M6	Not specified
CNA	Cisco	IOS	affected 15.3(3)M7	Not specified
CNA	Cisco	IOS	affected 15.3(3)M8	Not specified
CNA	Cisco	IOS	affected 15.3(3)M9	Not specified
CNA	Cisco	IOS	affected 15.3(3)M8a	Not specified
CNA	Cisco	IOS	affected 15.2(4)JN	Not specified
CNA	Cisco	IOS	affected 15.0(2)EZ	Not specified
CNA	Cisco	IOS	affected 15.2(1)EY	Not specified
CNA	Cisco	IOS	affected 15.0(2)EJ	Not specified
CNA	Cisco	IOS	affected 15.0(2)EJ1	Not specified
CNA	Cisco	IOS	affected 15.2(1)SY	Not specified
CNA	Cisco	IOS	affected 15.2(1)SY1	Not specified
CNA	Cisco	IOS	affected 15.2(1)SY0a	Not specified
CNA	Cisco	IOS	affected 15.2(1)SY2	Not specified
CNA	Cisco	IOS	affected 15.2(2)SY	Not specified
CNA	Cisco	IOS	affected 15.2(1)SY1a	Not specified
CNA	Cisco	IOS	affected 15.2(2)SY1	Not specified
CNA	Cisco	IOS	affected 15.2(2)SY2	Not specified
CNA	Cisco	IOS	affected 15.2(1)SY3	Not specified
CNA	Cisco	IOS	affected 15.2(1)SY4	Not specified
CNA	Cisco	IOS	affected 15.2(5)EX	Not specified

CNA	Cisco	IOS	affected 15.2(4)JAZ1	Not specified
CNA	Cisco	IOS	affected 15.0(2)EK	Not specified
CNA	Cisco	IOS	affected 15.0(2)EK1	Not specified
CNA	Cisco	IOS	affected 15.4(1)CG	Not specified
CNA	Cisco	IOS	affected 15.4(1)CG1	Not specified
CNA	Cisco	IOS	affected 15.4(2)CG	Not specified
CNA	Cisco	IOS	affected 15.2(2)EB	Not specified
CNA	Cisco	IOS	affected 15.2(2)EB1	Not specified
CNA	Cisco	IOS	affected 15.2(2)EB2	Not specified
CNA	Cisco	IOS	affected 15.5(1)T	Not specified
CNA	Cisco	IOS	affected 15.5(1)T1	Not specified
CNA	Cisco	IOS	affected 15.5(2)T	Not specified
CNA	Cisco	IOS	affected 15.5(1)T2	Not specified
CNA	Cisco	IOS	affected 15.5(1)T3	Not specified
CNA	Cisco	IOS	affected 15.5(2)T1	Not specified
CNA	Cisco	IOS	affected 15.5(2)T2	Not specified
CNA	Cisco	IOS	affected 15.5(2)T3	Not specified
CNA	Cisco	IOS	affected 15.5(2)T4	Not specified
CNA	Cisco	IOS	affected 15.5(1)T4	Not specified
CNA	Cisco	IOS	affected 15.2(2)EA	Not specified
CNA	Cisco	IOS	affected 15.2(2)EA1	Not specified
CNA	Cisco	IOS	affected 15.2(2)EA2	Not specified
CNA	Cisco	IOS	affected 15.2(3)EA	Not specified
CNA	Cisco	IOS	affected 15.2(4)EA	Not specified
CNA	Cisco	IOS	affected 15.2(4)EA1	Not specified
CNA	Cisco	IOS	affected 15.2(2)EA3	Not specified
CNA	Cisco	IOS	affected 15.2(4)EA3	Not specified
CNA	Cisco	IOS	affected 15.2(5)EA	Not specified
CNA	Cisco	IOS	affected 15.2(4)EA4	Not specified
CNA	Cisco	IOS	affected 15.2(4)EA5	Not specified
CNA	Cisco	IOS	affected 15.5(3)M	Not specified
CNA	Cisco	IOS	affected 15.5(3)M1	Not specified
CNA	Cisco	IOS	affected 15.5(3)M0a	Not specified
CNA	Cisco	IOS	affected 15.5(3)M2	Not specified
CNA	Cisco	IOS	affected 15.5(3)M3	Not specified
CNA	Cisco	IOS	affected 15.5(3)M4	Not specified

CNA	Cisco	IOS	affected 15.5(3)M4a	Not specified
CNA	Cisco	IOS	affected 15.5(3)M5	Not specified
CNA	Cisco	IOS	affected 15.3(3)JAA1	Not specified
CNA	Cisco	IOS	affected 15.0(2)SQD	Not specified
CNA	Cisco	IOS	affected 15.0(2)SQD1	Not specified
CNA	Cisco	IOS	affected 15.0(2)SQD2	Not specified
CNA	Cisco	IOS	affected 15.0(2)SQD3	Not specified
CNA	Cisco	IOS	affected 15.0(2)SQD4	Not specified
CNA	Cisco	IOS	affected 15.0(2)SQD5	Not specified
CNA	Cisco	IOS	affected 15.0(2)SQD6	Not specified
CNA	Cisco	IOS	affected 15.6(1)T	Not specified
CNA	Cisco	IOS	affected 15.6(2)T	Not specified
CNA	Cisco	IOS	affected 15.6(1)T0a	Not specified
CNA	Cisco	IOS	affected 15.6(1)T1	Not specified
CNA	Cisco	IOS	affected 15.6(2)T1	Not specified
CNA	Cisco	IOS	affected 15.6(1)T2	Not specified
CNA	Cisco	IOS	affected 15.6(2)T2	Not specified
CNA	Cisco	IOS	affected 15.6(1)T3	Not specified
CNA	Cisco	IOS	affected 15.3(1)SY	Not specified
CNA	Cisco	IOS	affected 15.3(1)SY1	Not specified
CNA	Cisco	IOS	affected 15.3(1)SY2	Not specified
CNA	Cisco	IOS	affected 15.6(3)M	Not specified
CNA	Cisco	IOS	affected 15.6(3)M1	Not specified
CNA	Cisco	IOS	affected 15.6(3)M0a	Not specified
CNA	Cisco	IOS	affected 15.6(3)M1b	Not specified
CNA	Cisco	IOS	affected 15.6(3)M2	Not specified
CNA	Cisco	IOS	affected 15.6(3)M2a	Not specified
CNA	Cisco	IOS	affected 15.2(4)EC1	Not specified
CNA	Cisco	IOS	affected 15.2(4)EC2	Not specified
CNA	Cisco	IOS	affected 15.3(3)JPC5	Not specified
CNA	Cisco	IOS	affected 15.4(1)SY	Not specified
CNA	Cisco	IOS	affected 15.4(1)SY1	Not specified
CNA	Cisco	IOS	affected 15.4(1)SY2	Not specified
CNA	Cisco	IOS	affected 15.5(1)SY	Not specified
CNA	Cisco	IOS	affected 15.3(3)JPR1	Not specified

CNA	Cisco	Cisco IOS XE Software	affected 3.2.0SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.1SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.2SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.3SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.4SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.5SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.6SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.7SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.8SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.9SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.10SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.11SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.0SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.2SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.1SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.0SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.1SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.2SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.2.3SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.0SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.1SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.2SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.3SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.4SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.5SE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.0SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.2SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.1SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.3SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.4SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.5SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.6SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.7SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.8SG	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.0E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.1E	Not specified

CNA	Cisco	Cisco IOS XE Software	affected 3.5.1E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.2E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.3E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.0E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.1E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.2aE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.2E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.3E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.4E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.5E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.6E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.5aE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.6.5bE	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.0SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.3.1SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.0SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.4.1SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.0E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.1E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.2E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.7.3E	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 3.5.0SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.1SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.2SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.3SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.4SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.5SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.5.6SQ	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.1.1	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.1.2	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.1.3	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 3.8.0E	Not specified

CNA	Cisco	Cisco IOS XE Software	affected 3.8.1E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.8.2E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.8.3E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.8.4E	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 16.5.1a	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 16.5.1b	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	Cisco	Cisco IOS XE Software	affected 3.9.0E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.9.1E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 3.9.2E	Not specified
CNA	Cisco	Cisco IOS XE Software	affected 17.11.99SW	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
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-
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-
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

Source	Time	Event
ADP	2022-03-03T00:00:00.000Z	CVE-2017-6738 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)