CVE-2017-6615

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

Summary

CVE	CVE-2017-6615
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-20 22:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS XE 3.16 could allow an authe

Risk And Classification

Problem Types: CWE-362 | CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xe	3.16.0cs	All	All	All
Operating System	Cisco	Ios Xe	3.16.0s	All	All	All
Operating System	Cisco	Ios Xe	3.16.1as	All	All	All
Operating System	Cisco	Ios Xe	3.16.1s	All	All	All
Operating System	Cisco	Ios Xe	3.16.2s	All	All	All
Operating System	Cisco	Ios Xe	3.16.0cs	All	All	All
Operating System	Cisco	Ios Xe	3.16.0s	All	All	All
Operating System	Cisco	Ios Xe	3.16.1as	All	All	All
Operating System	Cisco	Ios Xe	3.16.1s	All	All	All
Operating System	Cisco	Ios Xe	3.16.2s	All	All	All

References

Reference	Source
Cisco IOS XE Software CVE-2017-6615 Denial of Service Vulnerability	BID
Cisco IOS XE SNMP Race Condition Lets Remote Authenticated Users Cause the Target System to Restart - SecurityTracker	SECTRACK
Cisco IOS and IOS XE Software Simple Network Management Protocol Subsystem Denial of Service Vulnerability	CONFIRM
CVE Program record	CVE.ORG

NVD vulnerability detail NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**