CVE-2018-0299

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0299
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-21 11:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the Simple Network Management Protocol (SNMP) feature of Cisco NX-OS on the Cisco Nexus 4000 Seri

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 4001i	-	All	All	All
Hardware	Cisco	Nexus 4001i	-	All	All	All
Operating System	Cisco	Nx-os	4.1(2)e1(1r)	All	All	All
Operating System	Cisco	Nx-os	4.1\(2\)e1\(1r\)	All	All	All
Operating System	Cisco	Nx-os	4.1\(2\)e1\(1r\)	All	All	All

References

Reference
Cisco Nexus 4000 Series Switch Simple Network Management Protocol Polling Denial of Service Vulnerability
Cisco NX-OS Multiple Bugs Let Remote Users Deny Service and Execute Arbitrary Code and Let Remote Authenticated Users Gain Elevated
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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