



CVE-2017-3804

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

Summary

CVE	CVE-2017-3804
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-26 07:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A vulnerability in Intermediate System-to-Intermediate System (IS-IS) protocol packet processing of Cisco Nexus 5000, 600

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 5000	-	All	All	All
Hardware	Cisco	Nexus 5000	-	All	All	All
Hardware	Cisco	Nexus 6001	-	All	All	All
Hardware	Cisco	Nexus 6001	-	All	All	All
Hardware	Cisco	Nexus 6004	-	All	All	All
Hardware	Cisco	Nexus 6004	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Operating System	Cisco	Nx-os	7.1(3)n1(2.1)	All	All	All
Operating System	Cisco	Nx-os	7.1(3)n1(3.12)	All	All	All
Operating System	Cisco	Nx-os	7.1\3)n1\2.1\	All	All	All
Operating System	Cisco	Nx-os	7.1\3)n1\3.12\	All	All	All
Operating System	Cisco	Nx-os	7.3(2)n1(0.296)	All	All	All
Operating System	Cisco	Nx-os	7.3\2)n1\0.296\	All	All	All
Operating System	Cisco	Nx-os	8.0(1)s2	All	All	All
Operating System	Cisco	Nx-os	8.0\1\1)s2	All	All	All
Operating System	Cisco	Nx-os	7.1\3)n1\2.1\	All	All	All

Operating System	Cisco	Nx-os	7.1\3\n1\3.12\	All	All	All
Operating System	Cisco	Nx-os	7.3\2\n1\0.296\	All	All	All
Operating System	Cisco	Nx-os	8.0\1\s2	All	All	All

References

Reference
Cisco Nexus 5000/6000/7000 Series Switches IS-IS Packet Processing Flaw Lets Remote Users Cause the Target System to Reload - Security
Cisco Nexus 5000, 6000, and 7000 Series Switches Software IS-IS Packet Processing Denial of Service Vulnerability
Multiple Cisco Nexus Devices CVE-2017-3804 Denial of Service Vulnerability
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.