



CVE-2015-4296

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

Summary

CVE	CVE-2015-4296
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-19 23:59:00 UTC
Updated	2017-09-21 01:29:00 UTC
Description	Nexus Data Broker (NDB) on Cisco Nexus 3000 devices with software 6.0(2)A6(1) allows remote attackers to cause a denial of service (CPU usage) via a crafted packet.

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 3016	-	All	All	All
Hardware	Cisco	Nexus 3016	-	All	All	All
Hardware	Cisco	Nexus 3048	-	All	All	All
Hardware	Cisco	Nexus 3048	-	All	All	All
Hardware	Cisco	Nexus 3064	-	All	All	All
Hardware	Cisco	Nexus 3064	-	All	All	All
Hardware	Cisco	Nexus 31128pq	-	All	All	All
Hardware	Cisco	Nexus 31128pq	-	All	All	All
Hardware	Cisco	Nexus 3132q	-	All	All	All
Hardware	Cisco	Nexus 3132q	-	All	All	All
Hardware	Cisco	Nexus 3164q	-	All	All	All
Hardware	Cisco	Nexus 3164q	-	All	All	All
Hardware	Cisco	Nexus 3172	-	All	All	All
Hardware	Cisco	Nexus 3172	-	All	All	All
Hardware	Cisco	Nexus 3232c	-	All	All	All
Hardware	Cisco	Nexus 3232c	-	All	All	All
Hardware	Cisco	Nexus 3524	-	All	All	All

Hardware	Cisco	Nexus 3524	-	All	All	All
Hardware	Cisco	Nexus 3548	-	All	All	All
Hardware	Cisco	Nexus 3548	-	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a6(1)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a6(1)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a6(1)	All	All	All

References

Reference
Cisco Nexus 3000 Series NX-OS Java Connection Processing Flaw Lets Remote Users Cause the Target Service to Restart - SecurityTracke
Cisco Nexus 3000 Nexus Data Broker 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.