CVE-2014-3330

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

Summary

CVE	CVE-2014-3330
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-11 22:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	Cisco NX-OS 6.1(2)I2(1) on Nexus 9000 switches does not properly process packet-drop policy checks for logged packets,

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 9000	-	All	All	All
Hardware	Cisco	Nexus 9000	-	All	All	All
Operating System	Cisco	Nx-os	6.1(2)i2(1)	All	All	All
Operating System	Cisco	Nx-os	6.1\(2\)i2\(1\)	All	All	All
Operating System	Cisco	Nx-os	6.1\(2\)i2\(1\)	All	All	All

References

Reference	Source	Link
Cisco Nexus 9000 Series Switches Access List Bypass Vulnerability	CISCO	tools.
Cisco NX-OS Nexus 9000 Access List Logging Bug Lets Remote Users Bypass Access Control Lists - SecurityTracker	SECTRACK	www.
Cisco Nexus 9000 Series Switches CVE-2014-3330 Access List Security Bypass Vulnerability	BID	www.
IBM X-Force Exchange	XF	excha
Cisco Nexus 9000 Series Switches Access List Bypass Vulnerability	CONFIRM	tools.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

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**