



CVE-2012-4090

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

Summary

CVE	CVE-2012-4090
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-05 10:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	The management interface in Cisco NX-OS on Nexus 7000 devices allows remote authenticated users to obtain sensitive c

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7000 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 9-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 9-slot	-	All	All	All
Operating System	Cisco	Nx-os	-	All	All	All
Operating System	Cisco	Nx-os	-	All	All	All

References

Reference	Source	Link
Cisco Nexus 7000 Series Switches NX-OS CVE-2012-4090 Remote Information Disclosure Vulnerability	BID	www.se
98123	OSVDB	osvdb.c
IBM X-Force Exchange	XF	exchan
Cisco NX-OS Nexus 7000 Discloses Configuration Files to Remote Authenticated Users - SecurityTracker	SECTrack	www.se

Cisco Security Notice: Cisco Nexus 7000 Information Disclosure Vulnerability	CISCO	tools.cisco.com
Security Advisory SA55206 - Cisco NX-OS Configuration File Password Hashes Disclosure Security Issue - Secunia	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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