



CVE-2014-3295

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

Summary

CVE	CVE-2014-3295
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-14 04:26:00 UTC
Updated	2016-09-08 12:03:00 UTC
Description	The HSRP implementation in Cisco NX-OS 6.2(2a) and earlier allows remote attackers to bypass authentication and cause

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Nx-os	4.1.(2)	All	All	All
Operating System	Cisco	Nx-os	4.1.(3)	All	All	All
Operating System	Cisco	Nx-os	4.1.(4)	All	All	All
Operating System	Cisco	Nx-os	4.1.(5)	All	All	All
Operating System	Cisco	Nx-os	4.1.\(2\)	All	All	All
Operating System	Cisco	Nx-os	4.1.\(3\)	All	All	All
Operating System	Cisco	Nx-os	4.1.\(4\)	All	All	All
Operating System	Cisco	Nx-os	4.1.\(5\)	All	All	All
Operating System	Cisco	Nx-os	4.2(3)	All	All	All
Operating System	Cisco	Nx-os	4.2(4)	All	All	All
Operating System	Cisco	Nx-os	4.2(6)	All	All	All
Operating System	Cisco	Nx-os	4.2(8)	All	All	All
Operating System	Cisco	Nx-os	4.2.(2a)	All	All	All
Operating System	Cisco	Nx-os	4.2.\(2a\)	All	All	All
Operating System	Cisco	Nx-os	4.2\3\	All	All	All
Operating System	Cisco	Nx-os	4.2\4\	All	All	All
Operating System	Cisco	Nx-os	4.2\6\	All	All	All

Operating System	Cisco	Nx-os	4.2\8\	All	All	All
Operating System	Cisco	Nx-os	5.0(2a)	All	All	All
Operating System	Cisco	Nx-os	5.0(3)	All	All	All
Operating System	Cisco	Nx-os	5.0(5)	All	All	All
Operating System	Cisco	Nx-os	5.0\2a\	All	All	All
Operating System	Cisco	Nx-os	5.0\3\	All	All	All
Operating System	Cisco	Nx-os	5.0\5\	All	All	All
Operating System	Cisco	Nx-os	5.1(1a)	All	All	All
Operating System	Cisco	Nx-os	5.1(3)	All	All	All
Operating System	Cisco	Nx-os	5.1(4)	All	All	All
Operating System	Cisco	Nx-os	5.1(5)	All	All	All
Operating System	Cisco	Nx-os	5.1(6)	All	All	All
Operating System	Cisco	Nx-os	5.1\1a\	All	All	All
Operating System	Cisco	Nx-os	5.1\3\	All	All	All
Operating System	Cisco	Nx-os	5.1\4\	All	All	All
Operating System	Cisco	Nx-os	5.1\5\	All	All	All
Operating System	Cisco	Nx-os	5.1\6\	All	All	All
Operating System	Cisco	Nx-os	5.2(1)	All	All	All
Operating System	Cisco	Nx-os	5.2(3a)	All	All	All
Operating System	Cisco	Nx-os	5.2(4)	All	All	All
Operating System	Cisco	Nx-os	5.2(5)	All	All	All
Operating System	Cisco	Nx-os	5.2(7)	All	All	All
Operating System	Cisco	Nx-os	5.2(9)	All	All	All
Operating System	Cisco	Nx-os	5.2\1\	All	All	All
Operating System	Cisco	Nx-os	5.2\3a\	All	All	All
Operating System	Cisco	Nx-os	5.2\4\	All	All	All
Operating System	Cisco	Nx-os	5.2\5\	All	All	All
Operating System	Cisco	Nx-os	5.2\7\	All	All	All
Operating System	Cisco	Nx-os	5.2\9\	All	All	All
Operating System	Cisco	Nx-os	6.0(1)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)	All	All	All
Operating System	Cisco	Nx-os	6.0(3)	All	All	All
Operating System	Cisco	Nx-os	6.0(4)	All	All	All
Operating System	Cisco	Nx-os	6.0\1\	All	All	All
Operating System	Cisco	Nx-os	6.0\2\	All	All	All

Operating System	Cisco	Nx-os	6.0\3\	All	All	All
Operating System	Cisco	Nx-os	6.0\4\	All	All	All
Operating System	Cisco	Nx-os	6.1(1)	All	All	All
Operating System	Cisco	Nx-os	6.1(2)	All	All	All
Operating System	Cisco	Nx-os	6.1(3)	All	All	All
Operating System	Cisco	Nx-os	6.1(4)	All	All	All
Operating System	Cisco	Nx-os	6.1(4a)	All	All	All
Operating System	Cisco	Nx-os	6.1\1\	All	All	All
Operating System	Cisco	Nx-os	6.1\2\	All	All	All
Operating System	Cisco	Nx-os	6.1\3\	All	All	All
Operating System	Cisco	Nx-os	6.1\4a\	All	All	All
Operating System	Cisco	Nx-os	6.1\4\	All	All	All
Operating System	Cisco	Nx-os	6.2(2)	All	All	All
Operating System	Cisco	Nx-os	6.2\2\	All	All	All
Operating System	Cisco	Nx-os	4.1.\2\	All	All	All
Operating System	Cisco	Nx-os	4.1.\3\	All	All	All
Operating System	Cisco	Nx-os	4.1.\4\	All	All	All
Operating System	Cisco	Nx-os	4.1.\5\	All	All	All
Operating System	Cisco	Nx-os	4.2.\2a\	All	All	All
Operating System	Cisco	Nx-os	4.2\3\	All	All	All
Operating System	Cisco	Nx-os	4.2\4\	All	All	All
Operating System	Cisco	Nx-os	4.2\6\	All	All	All
Operating System	Cisco	Nx-os	4.2\8\	All	All	All
Operating System	Cisco	Nx-os	5.0\2a\	All	All	All
Operating System	Cisco	Nx-os	5.0\3\	All	All	All
Operating System	Cisco	Nx-os	5.0\5\	All	All	All
Operating System	Cisco	Nx-os	5.1\1a\	All	All	All
Operating System	Cisco	Nx-os	5.1\3\	All	All	All
Operating System	Cisco	Nx-os	5.1\4\	All	All	All
Operating System	Cisco	Nx-os	5.1\5\	All	All	All
Operating System	Cisco	Nx-os	5.1\6\	All	All	All
Operating System	Cisco	Nx-os	5.2\1\	All	All	All
Operating System	Cisco	Nx-os	5.2\3a\	All	All	All
Operating System	Cisco	Nx-os	5.2\4\	All	All	All
Operating System	Cisco	Nx-os	5.2\5\	All	All	All
Operating System	Cisco	Nx-os	5.2\7\	All	All	All

Operating System	Cisco	Nx-os	5.2\(/)	All	All	All
Operating System	Cisco	Nx-os	5.2\(/9)	All	All	All
Operating System	Cisco	Nx-os	6.0\(/1)	All	All	All
Operating System	Cisco	Nx-os	6.0\(/2)	All	All	All
Operating System	Cisco	Nx-os	6.0\(/3)	All	All	All
Operating System	Cisco	Nx-os	6.0\(/4)	All	All	All
Operating System	Cisco	Nx-os	6.1\(/1)	All	All	All
Operating System	Cisco	Nx-os	6.1\(/2)	All	All	All
Operating System	Cisco	Nx-os	6.1\(/3)	All	All	All
Operating System	Cisco	Nx-os	6.1\(/4a)	All	All	All
Operating System	Cisco	Nx-os	6.1\(/4)	All	All	All
Operating System	Cisco	Nx-os	6.2\(/2)	All	All	All
Operating System	Cisco	Nx-os	All	All	All	All
Operating System	Cisco	Nx-os	All	All	All	All

References			
Reference	Source	Link	
Cisco NX-OS Software HSRP Packet Parsing Denial of Service Vulnerability	BID	www.securityfocus.com/bid/100000	
Security Advisory SA59158 - Cisco NX-OS HSRP Packet Handling Denial of Service Vulnerability - Secunia	SECUNIA	secunia.com/advisories/59158	
Cisco NX-OS HSRP Processing Flaw Lets Remote Users Deny Service - SecurityTracker	SECTrack	www.securitytracker.com/id?1036800	
Cisco Security Notice: Cisco NX-OS Software HSRP Authentication Denial of Service Vulnerability	CISCO	tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SN-59158	
Alert Details - Security Center - Cisco Systems	CONFIRM	tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SN-59158	
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/cve/2016/0704	
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2016-0704	

No vendor comments have been submitted for this CVE.

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