



CVE-2014-3261

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-3261
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-26 00:25:00 UTC
Updated	2018-10-30 16:26:00 UTC
Description	Buffer overflow in the Smart Call Home implementation in Cisco NX-OS on Fabric Interconnects in Cisco Unified Computing

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Cisco	Cg-os	cg4	All
Operating System	Cisco	Cg-os	cg4(1)	All
Operating System	Cisco	Cg-os	cg4\{(1)	All
Operating System	Cisco	Cg-os	cg4	All
Operating System	Cisco	Cg-os	cg4\{(1)	All
Hardware	Cisco	Cgr 1120	-	All
Hardware	Cisco	Cgr 1120	-	All
Hardware	Cisco	Cgr 1240	-	All
Hardware	Cisco	Cgr 1240	-	All
Hardware	Cisco	Nexus 3016q	-	All
Hardware	Cisco	Nexus 3016q	-	All
Hardware	Cisco	Nexus 3048	-	All
Hardware	Cisco	Nexus 3048	-	All
Hardware	Cisco	Nexus 3064t	-	All
Hardware	Cisco	Nexus 3064t	-	All
Hardware	Cisco	Nexus 3064x	-	All
Hardware	Cisco	Nexus 3064x	-	All

Hardware	Cisco	Nexus 3548	-	All
Hardware	Cisco	Nexus 3548	-	All
Hardware	Cisco	Nexus 4001i	-	All
Hardware	Cisco	Nexus 4001i	-	All
Hardware	Cisco	Nexus 5000	-	All
Hardware	Cisco	Nexus 5000	-	All
Hardware	Cisco	Nexus 5010	-	All
Hardware	Cisco	Nexus 5010	-	All
Hardware	Cisco	Nexus 5010p Switch	-	All
Hardware	Cisco	Nexus 5010p Switch	-	All
Hardware	Cisco	Nexus 5020	-	All
Hardware	Cisco	Nexus 5020	-	All
Hardware	Cisco	Nexus 5020p Switch	-	All
Hardware	Cisco	Nexus 5020p Switch	-	All
Hardware	Cisco	Nexus 5548p	-	All
Hardware	Cisco	Nexus 5548p	-	All
Hardware	Cisco	Nexus 5548up	-	All
Hardware	Cisco	Nexus 5548up	-	All
Hardware	Cisco	Nexus 5596up	-	All
Hardware	Cisco	Nexus 5596up	-	All
Hardware	Cisco	Nexus 7000	-	All
Hardware	Cisco	Nexus 7000	-	All
Hardware	Cisco	Nexus 7000 10-slot	-	All
Hardware	Cisco	Nexus 7000 10-slot	-	All
Hardware	Cisco	Nexus 7000 18-slot	-	All
Hardware	Cisco	Nexus 7000 18-slot	-	All
Hardware	Cisco	Nexus 7000 9-slot	-	All
Hardware	Cisco	Nexus 7000 9-slot	-	All
Operating System	Cisco	Nx-os	-	All
Operating System	Cisco	Nx-os	4.1.(2)	All
Operating System	Cisco	Nx-os	4.1.\(2)	All
Operating System	Cisco	Nx-os	5.0	All
Operating System	Cisco	Nx-os	5.0(2)	All
Operating System	Cisco	Nx-os	5.0(2)n1(1)	All
Operating System	Cisco	Nx-os	5.0(2)n2(1)	All

Operating System	Cisco	Nx-os	5.0(2)n2(1a)	All
Operating System	Cisco	Nx-os	5.0(2a)	All
Operating System	Cisco	Nx-os	5.0(3)	All
Operating System	Cisco	Nx-os	5.0(3)n1(1)	All
Operating System	Cisco	Nx-os	5.0(3)n1(1a)	All
Operating System	Cisco	Nx-os	5.0(3)n1(1b)	All
Operating System	Cisco	Nx-os	5.0(3)n1(1c)	All
Operating System	Cisco	Nx-os	5.0(3)n2(1)	All
Operating System	Cisco	Nx-os	5.0(3)n2(2)	All
Operating System	Cisco	Nx-os	5.0(3)n2(2a)	All
Operating System	Cisco	Nx-os	5.0(3)n2(2b)	All
Operating System	Cisco	Nx-os	5.0(3)u1(1a)	All
Operating System	Cisco	Nx-os	5.0(3)u1(1b)	All
Operating System	Cisco	Nx-os	5.0(3)u1(1d)	All
Operating System	Cisco	Nx-os	5.0(3)u1(2)	All
Operating System	Cisco	Nx-os	5.0(3)u1(2a)	All
Operating System	Cisco	Nx-os	5.0(3)u2(1)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2a)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2b)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2c)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2d)	All
Operating System	Cisco	Nx-os	5.0(3)u3(1)	All
Operating System	Cisco	Nx-os	5.0(3)u3(2)	All
Operating System	Cisco	Nx-os	5.0(3)u3(2a)	All
Operating System	Cisco	Nx-os	5.0(3)u3(2b)	All
Operating System	Cisco	Nx-os	5.0(3)u4(1)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1a)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1b)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1c)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1d)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1e)	All
Operating System	Cisco	Nx-os	5.0(5)	All
Operating System	Cisco	Nx-os	5.0(2a)	All

Operating System	Cisco	Nx-os	5.0\2\	All
Operating System	Cisco	Nx-os	5.0\2\n1\1\	All
Operating System	Cisco	Nx-os	5.0\2\n2\1a\	All
Operating System	Cisco	Nx-os	5.0\2\n2\1\	All
Operating System	Cisco	Nx-os	5.0\3\	All
Operating System	Cisco	Nx-os	5.0\3\n1\1a\	All
Operating System	Cisco	Nx-os	5.0\3\n1\1b\	All
Operating System	Cisco	Nx-os	5.0\3\n1\1c\	All
Operating System	Cisco	Nx-os	5.0\3\n1\1\	All
Operating System	Cisco	Nx-os	5.0\3\n2\1\	All
Operating System	Cisco	Nx-os	5.0\3\n2\2a\	All
Operating System	Cisco	Nx-os	5.0\3\n2\2b\	All
Operating System	Cisco	Nx-os	5.0\3\n2\2\	All
Operating System	Cisco	Nx-os	5.0\3\u1\1a\	All
Operating System	Cisco	Nx-os	5.0\3\u1\1b\	All
Operating System	Cisco	Nx-os	5.0\3\u1\1d\	All
Operating System	Cisco	Nx-os	5.0\3\u1\2a\	All
Operating System	Cisco	Nx-os	5.0\3\u1\2\	All
Operating System	Cisco	Nx-os	5.0\3\u2\1\	All
Operating System	Cisco	Nx-os	5.0\3\u2\2a\	All
Operating System	Cisco	Nx-os	5.0\3\u2\2b\	All
Operating System	Cisco	Nx-os	5.0\3\u2\2c\	All
Operating System	Cisco	Nx-os	5.0\3\u2\2d\	All
Operating System	Cisco	Nx-os	5.0\3\u2\2\	All
Operating System	Cisco	Nx-os	5.0\3\u3\1\	All
Operating System	Cisco	Nx-os	5.0\3\u3\2a\	All
Operating System	Cisco	Nx-os	5.0\3\u3\2b\	All
Operating System	Cisco	Nx-os	5.0\3\u3\2\	All
Operating System	Cisco	Nx-os	5.0\3\u4\1\	All
Operating System	Cisco	Nx-os	5.0\3\u5\1a\	All
Operating System	Cisco	Nx-os	5.0\3\u5\1b\	All
Operating System	Cisco	Nx-os	5.0\3\u5\1c\	All
Operating System	Cisco	Nx-os	5.0\3\u5\1d\	All
Operating System	Cisco	Nx-os	5.0\3\u5\1e\	All
Operating System	Cisco	Nx-os	5.0\3\u5\1\	All
Operating System	Cisco	Nx-os	5.0\5\	All

Operating System	Cisco	Nx-os	5.1	All
Operating System	Cisco	Nx-os	5.1(1)	All
Operating System	Cisco	Nx-os	5.1(1a)	All
Operating System	Cisco	Nx-os	5.1(2)	All
Operating System	Cisco	Nx-os	5.1(3)	All
Operating System	Cisco	Nx-os	5.1\1a\	All
Operating System	Cisco	Nx-os	5.1\1\	All
Operating System	Cisco	Nx-os	5.1\2\	All
Operating System	Cisco	Nx-os	5.1\3\	All
Operating System	Cisco	Nx-os	5.2	All
Operating System	Cisco	Nx-os	5.2(1)	All
Operating System	Cisco	Nx-os	5.2(3)	All
Operating System	Cisco	Nx-os	5.2\1\	All
Operating System	Cisco	Nx-os	5.2\3\	All
Operating System	Cisco	Nx-os	-	All
Operating System	Cisco	Nx-os	4.1.\2\	All
Operating System	Cisco	Nx-os	5.0	All
Operating System	Cisco	Nx-os	5.0\2a\	All
Operating System	Cisco	Nx-os	5.0\2\	All
Operating System	Cisco	Nx-os	5.0\2\1\1\	All
Operating System	Cisco	Nx-os	5.0\2\2\1a\	All
Operating System	Cisco	Nx-os	5.0\2\2\1\	All
Operating System	Cisco	Nx-os	5.0\3\	All
Operating System	Cisco	Nx-os	5.0\3\1\1a\	All
Operating System	Cisco	Nx-os	5.0\3\1\1b\	All
Operating System	Cisco	Nx-os	5.0\3\1\1c\	All
Operating System	Cisco	Nx-os	5.0\3\1\1\	All
Operating System	Cisco	Nx-os	5.0\3\2\1\	All
Operating System	Cisco	Nx-os	5.0\3\2\2a\	All
Operating System	Cisco	Nx-os	5.0\3\2\2b\	All
Operating System	Cisco	Nx-os	5.0\3\2\2\	All
Operating System	Cisco	Nx-os	5.0\3\1\1a\	All
Operating System	Cisco	Nx-os	5.0\3\1\1b\	All
Operating System	Cisco	Nx-os	5.0\3\1\1d\	All
Operating System	Cisco	Nx-os	5.0\3\1\2a\	All

Operating System	Cisco	Nx-os	5.0(3)u1(2)	All
Operating System	Cisco	Nx-os	5.0(3)u2(1)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2a)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2b)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2c)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2d)	All
Operating System	Cisco	Nx-os	5.0(3)u2(2)	All
Operating System	Cisco	Nx-os	5.0(3)u3(1)	All
Operating System	Cisco	Nx-os	5.0(3)u3(2a)	All
Operating System	Cisco	Nx-os	5.0(3)u3(2b)	All
Operating System	Cisco	Nx-os	5.0(3)u3(2)	All
Operating System	Cisco	Nx-os	5.0(3)u4(1)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1a)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1b)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1c)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1d)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1e)	All
Operating System	Cisco	Nx-os	5.0(3)u5(1)	All
Operating System	Cisco	Nx-os	5.0(5)	All
Operating System	Cisco	Nx-os	5.1	All
Operating System	Cisco	Nx-os	5.1(1a)	All
Operating System	Cisco	Nx-os	5.1(1)	All
Operating System	Cisco	Nx-os	5.1(2)	All
Operating System	Cisco	Nx-os	5.1(3)	All
Operating System	Cisco	Nx-os	5.2	All
Operating System	Cisco	Nx-os	5.2(1)	All
Operating System	Cisco	Nx-os	5.2(3)	All
Hardware	Cisco	Unified Computing System 6120xp Fabric Interconnect	-	All
Hardware	Cisco	Unified Computing System 6120xp Fabric Interconnect	-	All
Hardware	Cisco	Unified Computing System 6140xp Fabric Interconnect	-	All
Hardware	Cisco	Unified Computing System 6140xp Fabric Interconnect	-	All
Hardware	Cisco	Unified Computing System 6248up Fabric Interconnect	-	All
Hardware	Cisco	Unified Computing System 6248up Fabric Interconnect	-	All
Hardware	Cisco	Unified Computing System 6296up Fabric Interconnect	-	All
Hardware	Cisco	Unified Computing System 6296up Fabric Interconnect	-	All
Operating System	Cisco	Unified Computing System Infrastructure And Unified Computing System Software	4.4(4)	All

Operating System	Cisco	Unified Computing System Infrastructure And Unified Computing System Software	1.4(1j)	All
Operating System	Cisco	Unified Computing System Infrastructure And Unified Computing System Software	1.4(1j)	All
Operating System	Cisco	Unified Computing System Infrastructure And Unified Computing System Software	1.4(1j)	All

References

Reference	Source	Link	Tags
Cisco Security Advisory: Multiple Vulnerabilities in Cisco NX-OS-Based Products	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report