Cisco Security Advisory

GNU Bash Environment Variable Command Injection Vulnerability

High

Advisory ID:	cisco-sa-20140926-bash
Last Updated:	2015 April 1 21:14 GMT
Published:	2014 September 26 01:00 GMT
Version1.29:	Final
CVSS Score:	Base - 7.5
Workarounds:	See below
Cisco Bug IDs:	CSCur01959 CSCur02931

CVE-2014-6271
CVE-2014-6277
CVE-2014-6278
CVE-2014-7169
CVE-2014-7186
CVE-2014-7187

Download CVRF
Download PDF
Email

Summary

On September 24, 2014, a vulnerability in the Bash shell was publicly announced. The vulnerability is related to the way in which shell functions are passed though environment variables. The vulnerability may allow an attacker to inject commands into a Bash shell, depending on how the shell is invoked. The Bash shell may be invoked by a number of processes including, but not limited to, telnet, SSH, DHCP, and scripts hosted on web servers.

All versions of GNU Bash starting with version 1.14 are affected by this vulnerability and the specific impact is determined by the characteristics of the process using the Bash shell. In the worst case, an unauthenticated remote attacker would be able to execute commands on an affected server. However, in most cases involving Cisco products, authentication is required before exploitation could be attempted.

A number of Cisco products ship with or use an affected version of the Bash shell. The Bash shell is a third-party software component that is part of the GNU software project and used by a number of software vendors. As of this version of the Security Advisory, there have been a number of vulnerabilities recently discovered in the Bash shell, and the investigation is ongoing. For vulnerable products, Cisco has included information on the product versions that will contain the fixed software, and the date these versions are expected to be published on the cisco.com download page. This advisory will be updated as additional information becomes available. Cisco may release free software updates that address this vulnerability if a product is determined to be affected by this vulnerability. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash

Affected Products

Cisco is currently investigating it's product line to determine which products may be affected and the extent of the impact of the vulnerability on it's products. Additional Cisco products will be added as the investigation progresses.

The following Cisco products are currently under investigation

None

Vulnerable Products

Customers interested in tracking the progress of any of the following bugs can visit the Cisco Bug Search Tool to view the defect details and optionally select *Save Bug* and activate the *Email Notification* feature to receive automatic notifications when the bug is updated. Fixed software may be obtained from cisco.com download page.

Products and services listed in the subsections below have had their exposure to this vulnerability confirmed. Additional information will be added to these sections as the investigation continues:

Product	Defect	Fixed releases availability
Network Application, Service, and Acceleration		
Cisco ACE Application Control Engine Module for the Cisco Catalyst 6500	CSCur02931	Contact TAC for upgrade options.
Cisco Application Control Engine (ACE10 and ACE20)	CSCur07312	Contact TAC for upgrade options.
Cisco Application Control Engine (ACE30/ ACE 4710)	CSCur02195	(A patch is available for vulnerable releases.) A5(3.1b) (30-Nov-14)
Cisco Application and Content Networking System (ACNS)	CSCur05564	5.5.37 (5-Dec-14)
Cisco DC Health Check	CSCur09963	DCAF 4.0 (Available)
Cisco GSS 4492R Global Site Selector	CSCur02747	4.1(3.0.7) (Available) 3.2(0.1.4) (Available)
Cisco NAC Appliance	CSCur03364	A patch file is available for vulnerable releases.
Cisco Smart Call Home	CSCur05551	A patch file is available for vulnerable releases.
Cisco Sourcefire Defense Center and Sensor Product	None	4.10 (Available) 5.2 (Available) 5.3 (Available)
Cisco Visual Quality Experience Server	CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Visual Quality Experience Tools Server	CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Wide Area Application Services (WAAS)	CSCur02917	A patch file is available for 4.4.x releases and 5.2.1b. 5.0.3h (Available) 5.1.1h (Available) 5.3.5c (25-Nov-14)
Network and Content Security Devices		
Cisco ASA CX and Cisco Prime Security Manager	CSCur01959	9.3.2.1 (Available)
Cisco Clean Access Manager	CSCur05566	A patch file is available for vulnerable releases.
Cisco FireSIGHT	CSCur05199	(A patch file is available for vulnerable releases.) 5.3.0.3 (30-Nov-2014) 5.3.1.1 (Available) 5.2.0.7 (Available) 4.10.3.10 (Available)
Cisco Identity Services Engine (ISE)	CSCur00532	1.3.0.876 (Available) 1.2.0 Patch 12 (Available) 1.2.1 Patch 3 (Available) 1.1.3 Patch 12 (12-Dec-14) 1.1.4 Patch 12 (12-Dec-14)
Cisco Intrusion Prevention System Solutions (IPS)	CSCur00552	7.1.9 (Available) 7.3.3 (Jan 2015)
Cisco IronPort Encryption Appliance	CSCur02831	(A patch file is available for vulnerable releases)
Cisco NAC Guest Server	CSCur05629	A patch file is available for vulnerable releases.
Cisco NAC Server	CSCur05575	A patch file is available for vulnerable releases.
Cisco Physical Access Gateway	CSCur05343	1.5.3 (15-Apr-2015)
Cisco Physical Access Manager	CSCur05357	1.5.2 (Available)
Cisco Secure Access Control Server (ACS)	CSCur00511	A patch is available for vulnerable releases.
Cisco Virtual Security Gateway for Microsoft Hyper-V	CSCur05042	is 5.2(1)VSG2(1.2a) (30-Nov-14)
Network Management and Provisioning		
Cisco Access Registrar Appliance Cisco Prime Access Registrar Appliance	CSCur10557	5.x (Available) 6.x (Available)
Cisco Application Networking Manager	CSCur06823	5.2.5 (Available)
Cisco MXE Series	CSCur05088	3.3.2. (Available)
Cisco Media Experience Engines (MXE)	CSCur05088	3.3.2. (Available)
Cisco NetFlow Collection Agent	CSCur05232	A patch file is available for vulnerable releases. 6.2 (Available 1-Jun-2015)
		A patch file is available for vulnerable

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

BLG Another Major Vulnerability Bashes Systems

IS GNU Bash Environment Variable Command Injection Vulnerability

IS GNU Bash Environment Variable String Value Handling Vulnerability

IS GNU Bash redir_stack Handling Stack-Based Buffer Overflow Vulnerability

IS GNU Bash Off-By-One Logic Parsing Arbitrary Code Execution Vulnerability

IS GNU Bash Environment Variable Function Definitions Processing Arbitrary Code Execution Vulnerability

IS GNU Bash Environment Variable Content Processing Arbitrary Code Execution Vulnerability

AMB Identifying and Mitigating Exploitation of the GNU Bash Environment Variable Command Injection Vulnerability

ST 31975

ST 31976

ST 31977

ST 31978

ST 31985

ST 32038

ST 32039

ST 32041

ST 32042

ST 32043

ST 32045

ST 32046

ST 32047

ST 32049

ST 32069

ST 32335

ST 32336

ST 32366

ST 34847

Show All 27...

Subscribe to Cisco Security Notifications

Subscribe

Cisco Network Analysis Module	CSCur05225	releases. 6.2 (Available 1-Jun-2015)
Cisco Prime Collaboration Assurance	CSCur04820	10.5 (Available) 10.6 (15-Dec-2014)
Cisco Prime Collaboration Deployment	CSCur07766	A patch is available for vulnerable releases 10.5.2 (31-Dec-2014)
Cisco Prime IP Express	CSCur05200	8.2.0.5 (31-Jan-2015)
Cisco Prime Infrastructure	CSCur05228	A patch is available for vulnerable releases 2.1.2 (available)
Cisco Prime LAN Management Solution	CSCur05125	LMS 4.2.5 (31-Dec-2014) via patch
Cisco Prime License Manager	CSCur05098	10.5.1 SU (available) 10.5.2 (31-Dec-2014)
Cisco Prime Network Registrar (CPNR) Jumpstart	CSCur05136	8.2.2.1 (Available) 8.1.3.3 (31-Jan-2015) 7.2.3.5 (31-Jan-2015)
Cisco Prime Network Services Controller	CSCur05617	PNSC 3.4.1 (Available)
Cisco Prime Service Catalog Virtual Appliance	CSCur10723	PSC 10.0-R2 (Available)
Cisco UCS Central	CSCur05093	1.2(1d) (Available)
Data Center Analytics Framework (DCAF)	CSCur09685	4.0 (available)
Digital Media Manager (DMM)	CSCur03217	Patch is available for the following releases: 5.3 - 5.3.6 5.3.6_RB1 - 5.3.6_RB2 5.4- 5.4.1 5.4.1_RB1 5.4.1_RB2
Local Collector Appliance (LCA)	CSCur05780	2.2.6.1 (Available) 2.2.7
Network Configuration and Change Management	CSCur05794	A patch file is available for vulnerable releases.
Prime Collaboration Provisioning	CSCur04871	A patch file is available for vulnerable releases.
Unified Communication Audit Tool (UCAT)	CSCur05121	Affected systems have been patched.
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 Series	CSCur04507	14.0.23 (Available) 15.0.24 (Available)
Cisco IOS-XE for ASR1k, ASR903, ISR4400, CSR1000v	CSCur02734	15.4(2)S2/XE3.12.2S (Available) 15.4(3)S1/XE3.13.1S (Available) 15.5(1)S/XE3.14.0S (30-Nov-2015) 15.4(1)S3/XE3.11.3S (30-Nov-2014) 15.3(3)S5/XE3.10.5S (31-Jan-2015) 15.2(4)S7/XE3.7.7S (27-Feb-2015)
Cisco IOS-XE for Catalyst 3k, 4k, AIR-CT5760, and Cisco RF Gateway 10 (RFGW-10)	CSCur03368	15.1(2)SG5/3.4.5SG (21-Nov-2014) 15.0(2)SG10/3.2.10SG (31-Dec-2014) 15.2(1)E1/3.6.1E (28-Nov-2014) 15.0(1)EZ5/3.3.5SE (Available)
Cisco MDS	CSCur01099	(A patch file is available for vulnerable releases.)
Cisco Nexus 1000 Virtual Supervisor Module (VSM)	CSCur04438	N1KV Vmware N1KV 5.2(1)SV3(1.2) (mid-November 2014) N1KV HyperV release 5.2(1)SM2(1.1) (1-Dec-2014)
Cisco Nexus 1010	CSCur04510	5.2(1)SP1(7.2) (Available)
Cisco Nexus 3000 / 3500	CSCur04934	6.0(2)U5(1) (Available) 6.0(2)U4(2) (Available) 6.0(2)U3(4) (Available) 6.0(2)U2(11Z) (Available)
Cisco Nexus 4000	CSCur05610	4.1(2)E1(1n) (1-Dec-2014)
Cisco Nexus 5000/6000	CSCur05017	Gold Coast MR8 5.2(1)N1(8b) (Available) Harbord Plus MR4(a) 6.0(2)N2(5a) (Available) Iluka MR4 7.0(5)N1(1) (Available)
Cisco Nexus 7000 Series Switches	CSCur04856	5.2(9a) (Available) 6.1(5a) (Available) 6.2(8b) (Available) 6.2(10) (Available)
Cisco Nexus 7000	CSCuq98748	5.2(9a) (Available) 6.1(5a) (Available) 6.2(8b) (Available) 6.2(10) (Available)
Cisco Nexus 9000 Switches	CSCur05011	6.1(2)I3(1) (Available)
Cisco Nexus 9000 running NxOS	CSCur02700	6.1(2)I2(1) (Available) 6.1(2)I2(2) (Available) 6.1(2)I2(2a) (Available) 6.1(2)I2(2b) (Available) 6.1(2)I2(3) (Available) 6.1(2)I3(1) (Available)
Cisco Nexus 9000	CSCur02102	11.0(1d) (Available)
Cisco OnePK All-in-One VM	CSCur04925	(Available - use vendor patch.)
Cisco Quantum SON Suite	CSCur05662	(Affected systems to be patched by 1-Feb-2015.)
Cisco Quantum Virtualized Packet Core	CSCur05662	(Affected systems to be patched by 1-Feb-2015.)
Cisco Service Control Engine 1010	CSCur05021	A patch file will be available for Cisco Service Control Engine 8000 by 30-Nov-14. A patch file will be available for Cisco Service Control Engine 10000 by 19-Dec-14.
Cisco Service Control Engine 8000	CSCur05021	A patch file will be available for Cisco Service Control Engine 8000 by 30-Nov-14. A patch file will be available for Cisco Service Control Engine 10000 by 19-Dec-14.
Cisco Virtual Switch Update Manager	CSCur12303	1.1 (Available)
IOS-XR for Cisco Network Convergence System (NCS) 6000	CSCur02177	5.2.3 (31-Dec-2014) 5.0.1 (SMU available 31-Nov-2014) 5.2.1 (SMU available 31-Nov-2014)
Routing and Switching - Small Business		
Cisco WAG310G Residential Gateway	CSCur05525	Contact TAC for upgrade options.
Unified Computing		
Cisco Standalone rack server CIMC	CSCur03816	1.4(3x/y) (25-Nov-14) 1.5(7d) (25-Nov-14) 2.0(3f/g) (25-Nov-14) 2.0(4x) (25-Nov-14) 2.0(2x) (25-Nov-14)
Cisco UCS Director	CSCur02877	A patch file is available for vulnerable releases.
Cisco UCS Invicta Appliance	CSCur05026	5.0.1.2 (Available)
Cisco UCS Manager	CSCur01379	3.0(1d) (Available) 2.2(3b) (Available) 2.2(2e) (Available) 2.2(1f) (Available) 2.1(3f) (Available) 2.0(5g) (Available)
Cisco USC Invicta Series Autosupport Portal	CSCur07304	5.0.1.2 (Available)
Cisco USC Invicta Series	CSCur04651	5.0.1.2 (Available)
Cisco Unified Computing System B-Series (Blade) Servers	CSCur05081	3.0.2 (15-Feb-2015)
Cisco Unified Computing System E-Series Blade Server	CSCur05553	3.0.1 (Available July 2015)
Cisco Virtual Security Gateway	CSCur95323	5.2(1)VSG2(1.2c) (Available)

Cisco Virtualization Experience Client 6215	CSCur05844	(A patch file is available for vulnerable releases.) 10.6 (22-Jan-15)
Voice and Unified Communications Devices		
Cisco Business Edition 3000 (BE3k)	CSCur08462	Contact TAC for upgrade options.
Cisco Emergency Responder	CSCur05434	Patch - Available (applicable to all previous CER version 8.x 9.x 10.x)
Cisco Finesse	CSCur02866	A patch file is available for vulnerable releases
Cisco Hosted Collaboration Mediation Fulfillment	CSCur05477	(A patch file is available for affected releases.)
Cisco IM and Presence Service (CUPS)	CSCur05454	(A patch file is available for affected releases.) 10.5.1 SU2 (Available)
Cisco IP Interoperability and Collaboration System (IPICS)	CSCur05245	IPICS 4.8.2
Cisco MediaSense	CSCur02875	9.1 ES (Available) 10.5SU (Patch Available) - Will work with ANY supported version of MS
Cisco Paging Server (Informacast)	CSCur04834	9.0.2 (Available)
Cisco SocialMiner	CSCur02880	(A patch file is available for affected releases.) 10.6(1) (17-Dec-2014)
Cisco Unified Communications Domain Manager	CSCur01180	A patch file is available for vulnerable releases.
Cisco Unified Communications Manager (CUCM)	CSCur00930	A patch file is available for vulnerable releases. 10.5(1.11011.1) (Available) 10.0(1.13012.1) (Available) 9.1(2.13060.1) (Available) 8.6(2.26147.1) (Available) 8.5(1.17131.2) (Available)
Cisco Unified Contact Center Express (UCCX)	CSCur02861	A patch file is available for vulnerable releases. 10.6(1) (3-Dec-2014)
Cisco Unified Intelligence Center (CUIC)	CSCur02891	A patch file is available for vulnerable releases. CUIC 11.0(1) (30-Jun-2015)
Cisco Unified Quick Connect	CSCur05412	Contact TAC for upgrade options.
Cisco Unity Connection (UC)	CSCur05328	A patch file is available for vulnerable releases. 8.6.2ES153 (Available) 9.1.2ES67 (Available) 10.5.1ES74 (Available) 8.5.1 (mid-December 2014)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco AutoBackup Server	CSCur09315	Shellshock-1.0.1 (for all DBDS Linux 5.x 6.x products) - Patch Available
Cisco D9036 Modular Encoding Platform	CSCur04504	V02.02.30 (Available)
Cisco Digital Media Manager (DMM)	CSCur03539	5.3.1 (Available) 5.3.7 (Available) 5.3.10 (Available) 5.3.11 (Available) 5.3.12 (Available) 5.5 (Available)
Cisco Digital Media Player (DMP) 4310	CSCur05628	5.3(6)RB(2P) (Available) 5.4(1)RB(2P) (Available)
Cisco Download Server (DLS) (RH Based)	CSCur09318	Shellshock-1.0.1 (for all DBDS Linux 5.x 6.x products) - Patch Available
Cisco Edge 300 Digital Media Player	CSCur02761	A patch (V1.6.0) file is available for vulnerable releases.
Cisco Edge 340 Digital Media Player	CSCur02751	1.1.0.4 1.2 (20-Dec-14)
Cisco Enterprise Content Delivery Service	CSCur02848	2.6.3 (Available)
Cisco Media Experience Engine (MXE)	CSCur04893	3.3.2. (Available)
Cisco PowerVu D9190 Conditional Access Manager (PCAM)	CSCur05774	1.1 (Available 30-Apr-2015)
Cisco Show and Share (SnS)	CSCur03539	5.3.1 (Available) 5.3.7 (Available) 5.3.10 (Available) 5.3.11 (Available) 5.3.12 (Available) 5.5 (Available)
Cisco StadiumVision Director	CSCur30139	StadiumVision: 3.2 build 520 (SP2) (Available)
Cisco StadiumVision Mobile Reporter	CSCur30167	2.0.1 (build 1) (Available)
Cisco StadiumVision Mobile Streamer	CSCur30155	2.0.1 (build 1) (Available)
Cisco TelePresence 1310	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence Conductor	CSCur02103	XC2.4.1 (Available) XC2.3.1 (Available)
Cisco TelePresence Exchange System (CTX)	CSCur05335	1.3.0.4.2.0 (7-Nov-2014)
Cisco TelePresence ISDN Link	CSCur05025	1.1.4 (Available)
Cisco TelePresence Manager (CTSMan)	CSCur05104	1.9.4 (Available)
Cisco TelePresence Multipoint Switch (CTMS)	CSCur05344	1.8.x (Patch file available) 1.9.7 (Available)
Cisco TelePresence Recording Server (CTRS)	CSCur05038	A patch file available for vulnerable releases.
Cisco TelePresence System 1000	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 1100	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 1300	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 3000 Series	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 500-32	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 500-37	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence TE Software (for E20 - EoL)	CSCur05162	4.1.5 (Available)
Cisco TelePresence TX 9000 Series	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence Video Communication Server (VCS/Expressway)	CSCur01461	X8.2.2 (available). X7.2.4 (available) X8.1.2 (available)
Cisco TelePresence endpoints (C series, EX series, MX series, MXG2 series, SX series) and the 10" touch panel	CSCur02591	5.1.13 (Available) 6.0.4 (Available) 6.1.4 (Available) 6.3.3 (Available) 7.2.1 (Available)
Cisco VDS Service Broker	CSCur05679	VDS-SB 1.4 (1-Dec-2014)
Cisco Video Distribution Suite for Internet Streaming VDS-IS	CSCur05320	3.3.1b112 (Available) 4.0.0b157 (Available) 4.1.0b036 (March 2015)

Cisco Video Surveillance Media Server	CSCur05423	(A patch file is available for affected releases.) 7.6.0 (15-Dec-14)
Cisco Virtual PGW 2200 Softswitch	CSCur05847	A patch file is available for vulnerable releases.
Cisco Hosted Services		
Cisco Cloud Services	CSCur05334	(Affected systems have been patched.)
Cisco Common Services Platform Collector	CSCur07881	Affected systems have been patched.
Cisco Intelligent Automation for Cloud	CSCur05134	4.1.0.81287.195 (Available)
Cisco Life Cycle Management (LCM)	CSCur05242	Affected systems have been patched.
Cisco NetAuthenticate	CSCur05632	Affected systems have been updated.
Cisco Proactive Network Operations Center	CSCur05856	(Affected systems have been patched.)
Cisco Smart Care	CSCur05638	1.13.2.1 (Available)
Cisco Universal Small Cell CloudBase	CSCur05647	(Affected systems have been patched.)
Cisco WebEx Node	CSCur10599	(Affected systems have been patched.
Network Performance Analytics (NPA)	CSCur05788	(Affected systems have been patched.)
Web Element Manager	CSCur09009	(Affected systems have been patched.)

Product	Defect	Fixed releases availability
Cable Modems		
Cisco Video Surveillance Media Server	CSCur05423	(A patch file is available for affected releases.) 7.6.0 (15-Dec-14)
Network Application, Service, and Acceleration		
Cisco ACE Application Control Engine Module for the Cisco Catalyst 6500	CSCur02931	Contact TAC for upgrade options.
Cisco Application Control Engine (ACE10 and ACE20)	CSCur07312	Contact TAC for upgrade options.
Cisco Application Control Engine (ACE30/ ACE 4710)	CSCur02195	(A patch is available for vulnerable releases.) A5(3.1b) (30-Nov-14)
Cisco Application and Content Networking System (ACNS)	CSCur05564	5.5.37 (5-Dec-14)
Cisco DC Health Check	CSCur09963	DCAF 4.0 (Available)
Cisco GSS 4492R Global Site Selector	CSCur02747	4.1(3.0.7) (Available) 3.2(0.1.4) (Available)
Cisco NAC Appliance	CSCur03364	A patch file is available for vulnerable releases.
Cisco Smart Call Home	CSCur05551	A patch file is available for vulnerable releases.
Cisco Visual Quality Experience Server	CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Visual Quality Experience Tools Server	CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Wide Area Application Services (WAAS)	CSCur02917	A patch file is available for 4.4.x releases and 5.2.1b. 5.0.3h (Available) 5.1.1h (Available) 5.3.5c (25-Nov-14)
Network and Content Security Devices		
Cisco ASA CX and Cisco Prime Security Manager	CSCur01959	9.3.2.1 (Available)
Cisco Clean Access Manager	CSCur05566	A patch file is available for vulnerable releases.
Cisco FireSIGHT	CSCur05199	(A patch file is available for vulnerable releases.) 5.3.0.3 (30-Nov-2014) 5.3.1.1 (Available) 5.2.0.7 (Available) 4.10.3.10 (Available)
Cisco Identity Services Engine (ISE)	CSCur00532	1.3.0.876 (Available) 1.2.0 Patch 12 (Available) 1.2.1 Patch 3 (Available) 1.1.3 Patch 12 (12-Dec-14) 1.1.4 Patch 12 (12-Dec-14)
Cisco Intrusion Prevention System Solutions (IPS)	CSCur00552	7.1.9 (Available) 7.3.3 (Jan 2015)
Cisco IronPort Encryption Appliance	CSCur02831	(A patch file is available for vulnerable releases)
Cisco NAC Guest Server	CSCur05629	A patch file is available for vulnerable releases.
Cisco NAC Server	CSCur05575	A patch file is available for vulnerable releases.
Cisco Physical Access Gateway	CSCur05343	1.5.3 (15-Apr-2015)
Cisco Physical Access Manager	CSCur05357	1.5.2 (Available)
Cisco Secure Access Control Server (ACS)	CSCur00511	A patch is available for vulnerable releases.
Cisco Virtual Security Gateway for Microsoft Hyper-V	CSCur05042	is 5.2(1)VSG2(1.2a) (30-Nov-14)
Network Management and Provisioning		
Cisco Access Registrar Appliance Cisco Prime Access Registrar Appliance	CSCur10557	5.x (Available) 6.x (Available)
Cisco Application Networking Manager	CSCur06823	5.2.5 (Available)
Cisco MXE Series	CSCur05088	3.3.2. (Available)
Cisco Media Experience Engines (MXE)	CSCur05088	3.3.2. (Available)
Cisco NetFlow Collection Agent	CSCur05232	A patch file is available for vulnerable releases. 6.2 (Available 1-Jun-2015)
Cisco Network Analysis Module	CSCur05225	A patch file is available for vulnerable releases. 6.2 (Available 1-Jun-2015)
Cisco Prime Collaboration Assurance	CSCur04820	10.5 (Available) 10.6 (15-Dec-2014)
Cisco Prime Collaboration Deployment	CSCur07766	A patch is available for vulnerable releases 10.5.2 (31-Dec-2014)
Cisco Prime IP Express	CSCur05200	8.2.0.5 (31-Jan-2015)
Cisco Prime Infrastructure	CSCur05228	A patch is available for vulnerable releases 2.1.2 (available)
Cisco Prime LAN Management Solution	CSCur05125	LMS 4.2.5 (31-Dec-2014) via patch
Cisco Prime License Manager	CSCur05098	10.5.1 SU (available) 10.5.2 (31-Dec-2014)
Cisco Prime Network Registrar (CPNR) Jumpstart	CSCur05136	8.2.2.1 (Available) 8.1.3.3 (31-Jan-2015) 7.2.3.5 (31-Jan-2015)
Cisco Prime Network Services Controller	CSCur05617	PNSC 3.4.1 (Available)
Cisco Prime Service Catalog Virtual Appliance	CSCur10723	PSC 10.0-R2 (Available)
Cisco UCS Central	CSCur05093	1.2(1d) (Available)
Data Center Analytics Framework (DCAF)	CSCur09685	4.0 (available)
Digital Media Manager (DMM)	CSCur03217	Patch is available for the following releases: 5.3 - 5.3.6 5.3.6_RB1 - 5.3.6_RB2 5.4- 5.4.1 5.4.1_RB1 5.4.1_RB2
Local Collector Appliance (LCA)	CSCur05780	2.2.6.1 (Available) 2.2.7
Network Configuration and Change Management	CSCur05794	A patch file is available for vulnerable releases.

Prime Collaboration Provisioning	CSCur04871	A patch file is available for vulnerable releases.
Unified Communication Audit Tool (UCAT)	CSCur05121	Affected systems have been patched.
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 Series	CSCur04507	14.0.23 (Available) 15.0.24 (Available)
Cisco IOS-XE for ASR1k, ASR903, ISR4400, CSR1000v	CSCur02734	15.4(2)S2/XE3.12.2S (Available) 15.4(3)S1/XE3.13.1S (Available) 15.5(1)S/XE3.14.0S (30-Nov-2015) 15.4(1)S3/XE3.11.3S (30-Nov-2014) 15.3(3)S5/XE3.10.5S (31-Jan-2015) 15.2(4)S7/XE3.7.7S (27-Feb-2015)
Cisco IOS-XE for Catalyst 3k, 4k, AIR-CT5760, and Cisco RF Gateway 10 (RFGW-10)	CSCur03368	15.1(2)SG5/3.4.5SG (21-Nov-2014) 15.0(2)SG10/3.2.10SG (31-Dec-2014) 15.2(1)E1/3.6.1E (28-Nov-2014) 15.0(1)EZ5/3.3.5SE (Available)
Cisco MDS	CSCur01099	(A patch file is available for vulnerable releases.)
Cisco Nexus 1000 Virtual Supervisor Module (VSM)	CSCur04438	N1KV Vmware N1KV 5.2(1)SV3(1.2) (mid-November 2014) N1KV HyperV release 5.2(1)SM2(1.1) (1-Dec-2014)
Cisco Nexus 1010	CSCur04510	5.2(1)SP1(7.2) (Available)
Cisco Nexus 3000 / 3500	CSCur04934	6.0(2)U5(1) (Available) 6.0(2)U4(2) (Available) 6.0(2)U3(4) (Available) 6.0(2)U2(11Z) (Available)
Cisco Nexus 4000	CSCur05610	4.1(2)E1(1n) (1-Dec-2014)
Cisco Nexus 5000/6000	CSCur05017	Gold Coast MR8 5.2(1)N1(8b) (Available) Harbord Plus MR4(a) 6.0(2)N2(5a) (Available) Iluka MR4 7.0(5)N1(1) (Available)
Cisco Nexus 7000 Series Switches	CSCur04856	5.2(9a) (Available) 6.1(5a) (Available) 6.2(8b) (Available) 6.2(10) (Available)
Cisco Nexus 7000	CSCuq98748	5.2(9a) (Available) 6.1(5a) (Available) 6.2(8b) (Available) 6.2(10) (Available)
Cisco Nexus 9000 Switches	CSCur05011	6.1(2)I3(1) (Available)
Cisco Nexus 9000 running NxOS	CSCur02700	6.1(2)I2(1) (Available) 6.1(2)I2(2) (Available) 6.1(2)I2(2a) (Available) 6.1(2)I2(2b) (Available) 6.1(2)I2(3) (Available) 6.1(2)I3(1) (Available)
Cisco Nexus 9000	CSCur02102	11.0(1d) (Available)
Cisco OnePK All-in-One VM	CSCur04925	(Available - use vendor patch.)
Cisco Quantum SON Suite	CSCur05662	(Affected systems to be patched by 1-Feb-2015.)
Cisco Quantum Virtualized Packet Core	CSCur05662	(Affected systems to be patched by 1-Feb-2015.)
Cisco Service Control Engine 1010	CSCur05021	A patch file will be available for Cisco Service Control Engine 8000 by 30-Nov-14. A patch file will be available for Cisco Service Control Engine 10000 by 19-Dec-14.
Cisco Service Control Engine 8000	CSCur05021	A patch file will be available for Cisco Service Control Engine 8000 by 30-Nov-14. A patch file will be available for Cisco Service Control Engine 10000 by 19-Dec-14.
Cisco Virtual Switch Update Manager	CSCur12303	1.1 (Available)
IOS-XR for Cisco Network Convergence System (NCS) 6000	CSCur02177	5.2.3 (31-Dec-2014) 5.0.1 (SMU available 31-Nov-2014) 5.2.1 (SMU available 31-Nov-2014)
Routing and Switching - Small Business		
Cisco WAG310G Residential Gateway	CSCur05525	Contact TAC for upgrade options.
Unified Computing		
Cisco Standalone rack server CIMC	CSCur03816	1.4(3x/y) (25-Nov-14) 1.5(7d) (25-Nov-14) 2.0(3f/g) (25-Nov-14) 2.0(4x) (25-Nov-14) 2.0(2x) (25-Nov-14)
Cisco UCS Director	CSCur02877	A patch file is available for vulnerable releases.
Cisco UCS Invicta Appliance	CSCur05026	5.0.1.2 (Available)
Cisco UCS Manager	CSCur01379	3.0(1d) (Available) 2.2(3b) (Available) 2.2(2e) (Available) 2.2(1f) (Available) 2.1(3f) (Available) 2.0(5g) (Available)
Cisco USC Invicta Series Autosupport Portal	CSCur07304	5.0.1.2 (Available)
Cisco USC Invicta Series	CSCur04651	5.0.1.2 (Available)
Cisco Unified Computing System B-Series (Blade) Servers	CSCur05081	3.0.2 (15-Feb-2015)
Cisco Unified Computing System E-Series Blade Server	CSCur05553	3.0.1 (Available July 2015)
Cisco Virtual Security Gateway	CSCur95323	5.2(1)VSG2(1.2c) (Available)
Cisco Virtualization Experience Client 6215	CSCur05844	(A patch file is available for vulnerable releases.) 10.6 (22-Jan-15)
Voice and Unified Communications Devices		
Cisco Business Edition 3000 (BE3k)	CSCur08462	Contact TAC for upgrade options.
Cisco Emergency Responder	CSCur05434	Patch - Available (applicable to all previous CER version 8.x 9.x 10.x)
Cisco Finesse	CSCur02866	A patch file is available for vulnerable releases
Cisco Hosted Collaboration Mediation Fulfillment	CSCur05477	(A patch file is available for affected releases.)
Cisco IM and Presence Service (CUPS)	CSCur05454	(A patch file is available for affected releases.) 10.5.1 SU2 (Available)
Cisco IP Interoperability and Collaboration System (IPICS)	CSCur05245	IPICS 4.8.2
Cisco MediaSense	CSCur02875	9.1 ES (Available) 10.5SU (Patch Available) - Will work with ANY supported version of MS
Cisco Paging Server (Informacast)	CSCur04834	9.0.2 (Available)
Cisco SocialMiner	CSCur02880	(A patch file is available for affected releases.) 10.6(1) (17-Dec-2014)
Cisco Unified Communications Domain Manager	CSCur01180	A patch file is available for vulnerable releases.
Cisco Unified Communications Manager (CUCM)	CSCur00930	A patch file is available for vulnerable releases. 10.5(1.11011.1) (Available) 10.0(1.13012.1) (Available) 9.1(2.13060.1) (Available) 8.6(2.26147.1) (Available) 8.5(1.17131.2) (Available)

Cisco Unified Contact Center Express (UCCX)	CSCur02861	A patch file is available for vulnerable releases. 10.6(1) (3-Dec-2014)
Cisco Unified Intelligence Center (CUIC)	CSCur02891	A patch file is available for vulnerable releases. CUIC 11.0(1) (30-Jun-2015)
Cisco Unified Quick Connect	CSCur05412	Contact TAC for upgrade options.
Cisco Unity Connection (UC)	CSCur05328	A patch file is available for vulnerable releases. 8.6.2ES153 (Available) 9.1.2ES67 (Available) 10.5.1ES74 (Available) 8.5.1 (mid-December 2014)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco AutoBackup Server	CSCur09315	Shellshock-1.0.1 (for all DBDS Linux 5.x 6.x products) - Patch Available
Cisco D9036 Modular Encoding Platform	CSCur04504	V02.02.30 (Available)
Cisco Digital Media Manager (DMM)	CSCur03539	5.3.1 (Available) 5.3.7 (Available) 5.3.10 (Available) 5.3.11 (Available) 5.3.12 (Available) 5.5 (Available)
Cisco Digital Media Player (DMP) 4310	CSCur05628	5.3(6)RB(2P) (Available) 5.4(1)RB(2P) (Available)
Cisco Download Server (DLS) (RH Based)	CSCur09318	Shellshock-1.0.1 (for all DBDS Linux 5.x 6.x products) - Patch Available
Cisco Edge 300 Digital Media Player	CSCur02761	A patch (V1.6.0) file is available for vulnerable releases.
Cisco Edge 340 Digital Media Player	CSCur02751	1.1.0.4 1.2 (20-Dec-14)
Cisco Enterprise Content Delivery Service	CSCur02848	2.6.3 (Available)
Cisco Media Experience Engine (MXE)	CSCur04893	3.3.2. (Available)
Cisco PowerVu D9190 Conditional Access Manager (PCAM)	CSCur05774	1.1 (Available 30-Apr-2015)
Cisco Show and Share (SnS)	CSCur03539	5.3.1 (Available) 5.3.7 (Available) 5.3.10 (Available) 5.3.11 (Available) 5.3.12 (Available) 5.5 (Available)
Cisco StadiumVision Director	CSCur30139	StadiumVision: 3.2 build 520 (SP2) (Available)
Cisco StadiumVision Mobile Reporter	CSCur30167	2.0.1 (build 1) (Available)
Cisco StadiumVision Mobile Streamer	CSCur30155	2.0.1 (build 1) (Available)
Cisco TelePresence 1310	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence Conductor	CSCur02103	XC2.4.1 (Available) XC2.3.1 (Available)
Cisco TelePresence Exchange System (CTX)	CSCur05335	1.3.0.4.2.0 (7-Nov-2014)
Cisco TelePresence ISDN Link	CSCur05025	1.1.4 (Available)
Cisco TelePresence Manager (CTSMan)	CSCur05104	1.9.4 (Available)
Cisco TelePresence Multipoint Switch (CTMS)	CSCur05344	1.8.x (Patch file available) 1.9.7 (Available)
Cisco TelePresence Recording Server (CTRS)	CSCur05038	A patch file available for vulnerable releases.
Cisco TelePresence System 1000	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 1100	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 1300	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 3000 Series	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 500-32	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence System 500-37	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence TE Software (for E20 - EoL)	CSCur05162	4.1.5 (Available)
Cisco TelePresence TX 9000 Series	CSCur05163	1.9.8 (Available) 6.1.5.1 (Available) 1.10.8.1 (Available)
Cisco TelePresence Video Communication Server (VCS/Expressway)	CSCur01461	X8.2.2 (available). X7.2.4 (available) X8.1.2 (available)
Cisco TelePresence endpoints (C series, EX series, MX series, MXG2 series, SX series) and the 10" touch panel	CSCur02591	5.1.13 (Available) 6.0.4 (Available) 6.1.4 (Available) 6.3.3 (Available) 7.2.1 (Available)
Cisco VDS Service Broker	CSCur05679	VDS-SB 1.4 (1-Dec-2014)
Cisco Video Distribution Suite for Internet Streaming VDS-IS	CSCur05320	3.3.1b112 (Available) 4.0.0b157 (Available) 4.1.0b036 (March 2015)
Cisco Virtual PGW 2200 Softswitch	CSCur05847	A patch file is available for vulnerable releases.
Cisco Hosted Services		
Cisco Cloud Services	CSCur05334	(Affected systems have been patched.)
Cisco Common Services Platform Collector	CSCur07881	Affected systems have been patched.
Cisco Intelligent Automation for Cloud	CSCur05134	4.1.0.81287.195 (Available)
Cisco Life Cycle Management (LCM)	CSCur05242	Affected systems have been patched.
Cisco NetAuthenticate	CSCur05632	Affected systems have been updated.
Cisco Proactive Network Operations Center	CSCur05856	(Affected systems have been patched.)
Cisco Smart Care	CSCur05638	1.13.2.1 (Available)
Cisco Universal Small Cell CloudBase	CSCur05647	(Affected systems have been patched.)
Cisco WebEx Node	CSCur10599	(Affected systems have been patched.
Network Performance Analytics (NPA)	CSCur05788	(Affected systems have been patched.)
Web Element Manager	CSCur09009	(Affected systems have been patched.)

Products Confirmed Not Vulnerable

Note: The following list includes Cisco applications that are intended to be installed on a customer-provided host (either a physical server or a virtual machine) with customer-installed operating systems. Those products may use the Bash shell as provided by the host operating system on which the Cisco product is installed. While those Cisco products do not directly include an affected version of Bash (and hence they are not impacted by this vulnerability), Cisco recommends that customers review their host operating system installation and perform any upgrades necessary to address this vulnerability, according to the operating system vendor recommendations and general operating system security best practices.

The following Cisco products have been analyzed and are not affected by this vulnerability:

Cable Modems

- Cisco Prime Network Registrar (CPNR)
- Digital Life RMS and Cisco Broadband Access Center Telco Wireless

Collaboration and Social Media

- Cisco Meetingplace
- Cisco WebEx Meetings Server (CWMS)
- Cisco WebEx Node for MCS
- Cisco WebEx Social

Endpoint Clients and Client Software

- Cisco IP Communicator
- Cisco Jabber Guest 10.0(2)
- Cisco NAC Agent for Mac
- Cisco NAC Agent for web
- Cisco UC Integration for Microsoft Lync
- Cisco Unified Personal Communicator
- Cisco Unified Video Advantage

Network Application, Service, and Acceleration

- Cisco Adaptive Security Appliance (ASA) Software
- Cisco Extensible Network Controller (XNC)
- Cisco Firewall Services Module
- Cisco Nexus Data Broker Cisco Extensible Network Controller (XNC)
- Cisco Openflow Agent
- Content Services Switch

Network and Content Security Devices

- Cisco ASA Content Security and Control (CSC) Security Services Module
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco Content Security Appliance Updater Servers
- Cisco Email Security Appliance (ESA)
- Cisco Ironport WSA
- Cisco Security Management Appliance (SMA)

Network Management and Provisioning

- Cisco Connected Grid Network Management System
- Cisco Insight reporter
- Cisco MATE (MATE collector, MATE Live, MATE Design)
- Cisco Media Gateway Controller Node Manager
- Cisco Multicast Manager
- Cisco Network Collector
- Cisco Prime Access Registrar
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Data Center Network Manager
- Cisco Prime Home
- Cisco Prime Network
- Cisco Prime Optical for SPs
- Cisco Prime Performance Manager for SPs
- Cisco Quantum Policy Suite (QPS)
- Cisco Security Manager
- Cisco TelePresence MPS Series
- Cisco Unified Provisioning Manager (CUPM)
- CiscoWorks Network Compliance Manager
- Network Profiler
- Security Module for Cisco Network Registrar
- Unified Communications Deployment Tools

Routing and Switching - Enterprise and Service Provider

- CRS-CGSE-PLIM CRS-CGSE-PLUS
- Cisco 1000 Series Connected Grid Routers
- Cisco ASR 9000 Series Integrated Service Module
- Cisco Application Policy Infrastructure Controller
- Cisco Broadband Access Center Telco Wireless
- Cisco Connected Grid Device Manager
- Cisco Connected Grid Routers (CGR)

- Cisco IOS
- Cisco IOS-XR running on
    - Cisco ASR 9000 Series Aggregation Services Routers
    - Cisco CRS Routers
    - Cisco XR 12000 Series Routers
- Cisco Metro Ethernet 1200 Series Access Devices
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco Prime Provisioning for SPs
- Cisco Service Control Application for Broadband
- Cisco Service Control Collection Manager
- Cisco Service Control Engine 2020
- Cisco Service Control Subscriber Manager
- Cisco VPN Acceleration Engine

Routing and Switching - Small Business

- Cisco RV180W Wireless-N Multifunction VPN Router
- Cisco Small Business AP500 Series Wireless Access Points
- Cisco Small Business ISA500 Series Integrated Security Appliances
- Cisco Small Business RV 120W Wireless-N VPN Firewall
- Cisco Small Business RV Series Routers 0xxv3
- Cisco Small Business RV Series Routers RV110W
- Cisco Small Business RV Series Routers RV130x
- Cisco Small Business RV Series Routers RV215W
- Cisco Small Business RV Series Routers RV220W
- Cisco Small Business RV Series Routers RV315W
- Cisco Small Business RV Series Routers RV320
- Cisco Sx220 switches
- Cisco WAP4410N Wireless-N Access Point

Unified Computing

- Cisco Common Services Platform Collector
- Cisco Intercloud Fabric
- Cisco UCS Series Fabric Extenders I/O Modules

Voice and Unified Communications Devices

- Cisco 190 ATA Series Analog Terminal Adaptor
- Cisco ATA 187 Analog Telephone Adaptor
- Cisco Agent Desktop for Cisco Unified Contact Center Express
- Cisco Agent Desktop
- Cisco Broadband Access Center for Cable Tools Suite 4.1 Cisco Broadband Access Center for Cable Tools Suite 4.2 Cisco Prime Cable Provisioning Tools Suite 5.0 Cisco Prime Cable Provisioning Tools Suite 5.1
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco Desktop Collaboration Experience DX650
- Cisco Desktop Collaboration Experience DX70 and DX80
- Cisco H.323 Signaling Interface
- Cisco IP Phone 8800 Series
- Cisco Jabber for Windows
- Cisco MS200X Ethernet Access Switch
- Cisco PGW 2200 Softswitch
- Cisco Packaged Contact Center Enterprise
- Cisco Remote Silent Monitoring
- Cisco SPA112 2-Port Phone Adapter
- Cisco SPA122 ATA with Router
- Cisco SPA232D Multi-Line DECT ATA
- Cisco SPA50X Series IP Phones
- Cisco SPA51X Series IP Phones
- Cisco SPA525G2 5-Line IP Phone
- Cisco SPA8000 8-port IP Telephony Gateway
- Cisco SPA8800 IP Telephony Gateway with 4 FXS and 4 FXO Ports
- Cisco Sx300 switches
- Cisco Sx500 Switches
- Cisco TAPI Service Provider (TSP)
- Cisco Unified 3900 series IP Phones
- Cisco Unified 6900 series IP Phones
- Cisco Unified 6911 IP Phones

- Cisco Unified 6945 IP Phones
- Cisco Unified 7800 series IP Phones
- Cisco Unified 8961 IP Phone
- Cisco Unified 9951 IP Phone
- Cisco Unified 9971 IP Phone
- Cisco Unified Attendant Console Advanced
- Cisco Unified Attendant Console Business Edition
- Cisco Unified Attendant Console Department Edition
- Cisco Unified Attendant Console Enterprise Edition
- Cisco Unified Attendant Console Premium Edition
- Cisco Unified Attendant Console Standard Edition
- Cisco Unified Client Services Framework
- Cisco Unified Communications Sizing Tool
- Cisco Unified Communications Widgets Click To Call
- Cisco Unified Contact Center Enterprise
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified IP Conference Phone 8831
- Cisco Unified IP Phone 7900 Series
- Cisco Unified Integration for IBM Sametime
- Cisco Unified Intelligence Center
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified Operations Manager (CUOM)
- Cisco Unified SIP Proxy
- Cisco Unified Service Monitor
- Cisco Unified Service Statistics Manager
- Cisco Unified Web Interaction Manager
- Cisco Unified Wireless IP Phone
- Cisco Unified Workforce Optimization
- Cisco Unity Express
- Cisco Universal Small Cell RAN Management System Wireless
- Cisco Virtualization Experience Media Engine
- xony VIM/CCDM/CCMP

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco AnyRes Live (CAL)
- Cisco AnyRes VOD (CAV)
- Cisco Command 2000 Server (cmd2k) (RH Based)
- Cisco Command 2000 Server (cmd2k)
- Cisco Common Download Server (CDLS)
- Cisco D9034-S Encoder
- Cisco D9054 HDTV Encoder
- Cisco D9804 Multiple Transport Receiver
- Cisco D9824 Advanced Multi Decryption Receiver
- Cisco D9854/D9854-I Advanced Program Receiver
- Cisco D9858 Advanced Receiver Transcoder
- Cisco D9859 Advanced Receiver Transcoder
- Cisco D9865 Satellite Receiver
- Cisco DCM Series 990x-Digital Content Manager
- Cisco DNCS Application Server (AppServer)
- Cisco Digital Network Control System (DNCS)
- Cisco Digital Transport Adapter Control System (DTACS)
- Cisco Download Server (DLS)
- Cisco Explorer Control Suite (ECS)
- Cisco Explorer Controller (EC)
- Cisco IPTV Service Delivery System (ISDS)
- Cisco IPTV
- Cisco International Digital Network Control System (iDNCS)
- Cisco Internet Streamer CDS
- Cisco Jabber Video for TelePresence (Movi)
- Cisco Jabber for TelePresence (Movi)
- Cisco Linear Stream Manager
- Cisco Model D9485 DAVIC QPSK
- Cisco Powerkey CAS Gateway (PCG)
- Cisco Powerkey Encryption Server (PKES)
- Cisco Remote Conditional Access System (RCAS)
- Cisco Remote Network Control System (RNCS)
- Cisco TelePresence Advanced Media Gateway Series
- Cisco TelePresence Content Server (TCS)
- Cisco TelePresence IP Gateway Series
- Cisco TelePresence IP VCR Series
- Cisco TelePresence ISDN GW 3241
- Cisco TelePresence ISDN GW MSE 8321
- Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)
- Cisco TelePresence MXP Software
- Cisco TelePresence Management Suite (TMS)
- Cisco TelePresence Management Suite Analytics Extension (TMSAE)
- Cisco TelePresence Management Suite Extension (TMSXE)
- Cisco TelePresence Management Suite Extension for IBM
- Cisco TelePresence Management Suite Provisioning Extension
- Cisco TelePresence Serial Gateway Series
- Cisco TelePresence Server 8710, 7010
- Cisco TelePresence Server on Multiparty Media 310, 320
- Cisco TelePresence Server on Virtual Machine
- Cisco TelePresence Supervisor MSE 8050
- Cisco Transaction Encryption Device (TED)
- Cisco Video Surveillance 3000 Series IP Cameras
- Cisco Video Surveillance 4000 Series High-Definition IP Cameras
- Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras
- Cisco Video Surveillance 6000 Series IP Cameras
- Cisco Video Surveillance 7000 Series IP Cameras
- Cisco Video Surveillance PTZ IP Cameras
- Cisco Videoscape Back Office (VBO)
- Cisco Videoscape Conductor
- Cisco Videoscape Distribution Suite Transparent Caching
- Cloud Object Store (COS)
- D9859 Advanced Receiver Transcoder
- Digital Media Player(DMP) 4400 Digital Media Player(DMP) 4310
- Media Services Interface
- Tandberg Codian ISDN GW 3210/3220/3240
- Tandberg Codian MSE 8320 model
- VDS-Recorder
- VDS-TV Caching GW
- VDS-TV Streamer
- VDS-TV Vault

Wireless

- Cisco Aironet Access Points running Cisco IOS
- Cisco Meraki Cloud Managed Indoor Access Points
- Cisco Meraki Cloud-Managed Outdoor Access Points
- Cisco Meraki MS Access Switches
- Cisco Mobility Services Engine (MSE)
- Cisco RF Gateway 1 (RFGW-1)
- Cisco Wireless Control System (WCS)
- Cisco Wireless LAN Controller (WLC)
- Cisco Wireless Location Appliance (WLA)

Cisco Hosted Services

- Business Video Services Automation Software (BV)
- Cisco Cloud Email Security
- Cisco Cloud and Systems Management
- Cisco Connected Analytics For Collaboration
- Cisco Connected Analytics for Network Deployment (CAND)
- Cisco Install Base Management (IBM)
- Cisco One View
- Cisco Registered Envelope Service (CRES)
- Cisco SLIM
- Cisco Serial Number Assessment Service (SNAS)
- Cisco Services Provisioning Platform (SPP) for MSA
- Cisco Smart Net Total Care (SNTC)
- Cisco Unified Services Delivery Platform (CUSDP)
- Cisco Universal Small Cell 5000 Series
- Cisco Universal Small Cell 7000 Series
- Cisco WebEx Meeting Clients and Productivity Tools
- Cisco WebEx Messenger Service
- Cisco WebEx WebOffice Workspace
- IC Capture
- IMS
- Partner Support Service (PSS) 1.x
- SI component of Partner Support Service

- Small Cell Factory Recovery
- Smart Net Total Care
- WebEx Connect
- WebEx Event Center, Meeting Center, Training Center, and Sales Center
- WebEx PCNow
- WebEx QuickBooks
- WebEx11 Application Server

Details

The bash shell allows shell variables and functions to be exported to a child from its parent through the process environment. Function definitions are passed using environment variables that share the name of the function and start with `() {`.

The child bash process does not stop processing and executing code after processing the closing brace `}` which is passed in the function definition. An attacker could define a function variable such as: `FUNCT=() { ignored; }; /bin/id` to execute /bin/id when the environment is imported into the child process.

The impact of this vulnerability on Cisco products may vary depending on the affected product because some attack vectors such as SSH, require successful authentication to be exploited and may not result in any additional privileges granted to the user.

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) IDs CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277 and CVE-2014-6278.

Several software tools have been created to help administrators identify if the version of Bash running on their platforms has been fixed. Several of these tools provide false positive results or crash the Bash shell. The information provided for each bug ID in the Cisco Bug Search Tool identifies the versions of software that contain the fixed code and should be used to determine if a product is vulnerable.

Workarounds

There are no mitigations for this vulnerability that can be performed directly on affected systems. However, the following network based mitigations may be of use to some customers.

- Cisco Intrusion Protection System (IPS) signature 4689-0 has been created and is available in release S824
- Cisco Sourcefire has published Snort signatures 31975-31977, 31985, 32038-32039, 32041-32043, 32045-32047, and 32049 to detect and protect networks against the Bash vulnerability

Cisco has published an Event Response for this vulnerability:
http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Bash_09252014.html

Mitigations that can be deployed on Cisco devices in a network are available in the Cisco Applied Intelligence companion document for this advisory:
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=35836

Fixed Software

Cisco will be providing software upgrades for vulnerable products. Information regarding the fix, including software versions that contain fixes can be found by referencing the Cisco bug ID from the list of vulnerable products and entering it in the Cisco Bug Search Tool.

When considering software upgrades, customers are advised to consult the release notes of the bug and the Cisco Security Advisories, Responses, and Notices archive at http://www.cisco.com/go/psirt and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Exploitation and Public Announcements

This vulnerability was reported by Stephane Chazelas and released by the GNU foundation on September 24, 2014.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash

---

Revision History

Revision 1.29	2015-April-01	Updated Fixed Software table and Products Confirmed Not Vulnerable sections.
Revision 1.28	2015-March-02	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.27	2015-January-12	Updated Fixed Software table.
Revision 1.26	2014-December-05	Updated Fixed Software table.
Revision 1.25	2014-November-24	Updated Fixed Software table.
Revision 1.24	2014-November-22	Updated Fixed Software table.
Revision 1.23	2014-November-20	Updated Fixed Software table.
Revision 1.22	2014-November-18	Updated Fixed Software table.
Revision 1.21	2014-November-13	Updated Fixed Software table.
Revision 1.20	2014-November-12	Updated Fixed Software table.
Revision 1.19	2014-November-10	Updated Fixed Software table.
Revision 1.18	2014-November-07	Updated Fixed Software table.
Revision 1.17	2014-November-06	Updated Fixed Software table.
Revision 1.16	2014-November-05	Updated Fixed Software table.
Revision 1.15	2014-November-04	Updated Fixed Software table.
Revision 1.14	2014-November-03	Added Fixed Software table.
Revision 1.13	2014-October-22	Updated the Products Confirmed Not Vulnerable section.
Revision 1.12	2014-October-15	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.11	2014-October-10	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.10	2014-October-09	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.9	2014-October-08	Updated details on where to find fix information, details on testing tools, and the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.8	2014-October-06	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.7	2014-October-03	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.6	2014-October-02	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
		Updated the Affected Products, Vulnerable

Revision 1.5	2014-October-01	Products, and Products Confirmed Not Vulnerable sections.
Revision 1.4	2014-September-30	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.3	2014-September-29	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.2	2014-September-27	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.1	2014-September-26	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.0	2014-September-26	Initial public release.
