GNU Bash環境変数コマンドインジェクションの脆弱性

アドバイザリーID : cisco-sa-20140926-bash
初公開日 : 2014-09-26 01:00
最終更新日 : 2015-04-01 21:14
バージョン 1.29 : Final
CVSSスコア : 7.5
回避策 : No Workarounds available
Cisco バグ ID : CSCur02931 CSCur01959

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

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

2014年9月24日、Bashシェルの脆弱性が公表されました。この脆弱性は、環境変数を介してシェル関数が渡される方法に関連しています。この脆弱性により、攻撃者はシェルの起動方法に応じて、Bashシェルにコマンドを挿入できる可能性があります。Bashシェルは、telnet、SSH、DHCP、Webサーバ上でホストされるスクリプトなど、さまざまなプロセスによって起動される可能性があります。

バージョン1.14以降のすべてのバージョンのGNU Bashは、この脆弱性の影響を受けます。具体的な影響は、Bashシェルを使用するプロセスの特性によって決まります。最悪のケースでは、認証されていないリモートの攻撃者が影響を受けるサーバでコマンドを実行する可能性があります。ただし、シスコ製品に関連するほとんどのケースでは、悪用を試みる前に認証が必要です。

多くのシスコ製品が、Bashシェルの該当バージョンを搭載しているか、使用しています。Bashシェルは、GNUソフトウェアプロジェクトの一部であるサードパーティのソフトウェアコンポーネントで、多くのソフトウェアベンダーによって使用されています。このバージョンのセキュリティアドバイザリでは、最近Bashシェルで多数の脆弱性が発見され、現在調査中です。脆弱性が存在する製品については、修正済みソフトウェアが含まれる製品のバージョンに関する情報と、これらのバージョンが cisco.comダウンロードページで公開される予定の日付が記載されていますを参照。このアドバイザリは追加情報が入手可能になった時点で更新されます。シスコは、製品がこの脆弱性の影響を受けると判断した場合、この脆弱性に対処する無償のソフトウェアアップ

デートをリリースする可能性があります。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash

該当製品

シスコでは現在、影響を受ける可能性のある製品と、その製品に対する脆弱性の影響の程度を判断するために、シスコの製品ラインを調査中です。調査の進行に伴い、シスコ製品が追加されます。

次のシスコ製品は現在調査中です

なし

脆弱性のある製品

次のバグの進行状況を追跡したいお客様は、 Cisco Bug Search Toolを使用して不具合の詳細を確認し、オプションで Save Bugを選択して Email Notification機能を有効にすると、バグが更新されたときに自動的に通知を受け取ることができます。修正済みソフトウェアは、cisco.com download pageから入手できます。

次のサブセクションに記載されている製品およびサービスは、この脆弱性の影響を受けることが確認されています。調査の進行に伴い、これらのセクションに追加情報が追加されます。

製品	Defect	Fixed releases availability
ネットワーク アプリケーション、サービス、およびアクセラレーション		
Cisco Catalyst 6500用Cisco ACE Application Control Engineモジュール	0.CSCur02931	アップグレードオプションについては、TACにお問い合わせください。
Cisco Application Control Engine (ACE10 and ACE20)	0.CSCur07312	アップグレードオプションについては、TACにお問い合わせください。
Cisco Application Control Engine（ACE30/ACE 4710）	0.CSCur02195	（脆弱性のあるリリースに対してパッチが提供されています）。 A5(3.1b)（11月30日、14日）
Cisco Application and Content Networking System（ACNS）	0.CSCur05564	5.5.37（12月14日）
Cisco DC Health Check	0.CSCur09963	DCAF 4.0（入手可能）
Cisco GSS 4492Rグローバルサイトセレクタ	0.CSCur02747	4.1(3.0.7)（入手可能） 3.2(0.1.4)（入手可能）
Cisco NAC アプライアンス	0.CSCur03364	脆弱性のあるリリースのパッチ ファイルが利用可能。

Cisco Smart Call Home	0.CSCur05551	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco Sourcefire Defense Centerおよびセンサー製品	なし	4.10 (Available) 5.2 (Available) 5.3 (Available)
Cisco Visual Quality Experience Server	0.CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Visual Quality Experience Tools Server	0.CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Wide Area Application Services（WAAS）	0.CSCur02917	パッチファイルは、4.4.xリリースと5.2.1bで使用できます。 5.0.3h（入手可能） 5.1.1h（入手可能） 5.3.5c（2014年11月25日）
ネットワークおよびコンテンツ セキュリティ デバイス		
Cisco ASA CX と Cisco Prime Security Manager	0.CSCur01959	9.3.2.1（入手可能）
Cisco Clean Access Manager	0.CSCur05566	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco FireSIGHT	0.CSCur05199	（脆弱性のあるリリースにはパッチファイルが用意されています）。 5.3.0.3（2014年11月30日） 5.3.1.1（入手可能） 5.2.0.7（入手可能） 4.10.3.10（入手可能）
Cisco Identity Services Engine（ISE）	0.CSCur00532	1.3.0.876（入手可能） 1.2.0パッチ12（入手可能） 1.2.1パッチ3（入手可能） 1.1.3パッチ12（12月14日） 1.1.4パッチ12（12月14日）
シスコ侵入防御システム（IPS）	0.CSCur00552	7.1.9（入手可能） 7.3.3（2015年1月）
Cisco IronPort暗号化アプライアンス	0.CSCur02831	（脆弱性のあるリリースにはパッチファイルを使用できます）
Cisco NAC Guest Server	0.CSCur05629	脆弱性のあるリリースのパッチ ファ

		イルが利用可能。
Cisco NAC Server	0.CSCur05575	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco Physical Accessゲートウェイ	0.CSCur05343	1.5.3 (15-Apr-2015)
Cisco Physical Access Manager	0.CSCur05357	1.5.2（入手可能）
Cisco Secure Access Control Server（ACS）	0.CSCur00511	A patch is available for vulnerable releases.
Cisco Virtual Security Gateway for Microsoft Hyper-V	0.CSCur05042	5.2(1)VSG2(1.2a)（14年11月30日）
ネットワーク管理とプロビジョニング		
Cisco Access Registrarアプライアンス Cisco Prime Access Registrarアプライアンス	0.CSCur10557	5.x（入手可能） 6.x（入手可能）
Cisco Application Networking Manager	0.CSCur06823	5.2.5（入手可能）
Cisco MXEシリーズ	0.CSCur05088	3.3.2.（入手可能）
Cisco Media Experience Engines（MXE）	0.CSCur05088	3.3.2.（入手可能）
Cisco NetFlow Collection Agent	0.CSCur05232	脆弱性のあるリリースのパッチ ファイルが利用可能。 6.2（2015年6月1日から利用可能）
Cisco Network Analysis Module	0.CSCur05225	脆弱性のあるリリースのパッチ ファイルが利用可能。 6.2（2015年6月1日から利用可能）
Cisco Prime Collaboration Assurance	0.CSCur04820	10.5 (Available) 10.6（2014年12月15日）
Cisco Prime Collaboration Deployment	0.CSCur07766	A patch is available for vulnerable releases 10.5.2（2014年12月31日）
Cisco Prime IP Express	0.CSCur05200	8.2.0.5（2015年1月31日）
Cisco Prime Infrastructure	0.CSCur05228	A patch is available for vulnerable releases 2.1.2（使用可能）
Cisco Prime LAN Management Solution	0.CSCur05125	パッチによるLMS 4.2.5（2014年12月31日）
Cisco Prime License Manager	0.CSCur05098	10.5.1 SU（入手可能） 10.5.2（2014年12月31日）

Cisco Prime Network Registrar(CPNR)Jumpstart	0.CSCur05136	8.2.2.1（入手可能） 8.1.3.3（2015年1月31日） 7.2.3.5（2015年1月31日）
Cisco Prime Network Services Controller	0.CSCur05617	PNSC 3.4.1（入手可能）
Cisco Prime サービス カタログ仮想アプライアンス	0.CSCur10723	PSC 10.0-R2（入手可能）
Cisco UCS Central	0.CSCur05093	1.2(1d)（入手可能）
Data Center Analytics Framework（DCAF）	0.CSCur09685	4.0（利用可能）
デジタルメディアマネージャ(DMM)	0.CSCur03217	パッチは次のリリースで利用可能です。 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）	0.CSCur05780	2.2.6.1（入手可能） 2.2.7
ネットワーク構成と変更管理	0.CSCur05794	脆弱性のあるリリースのパッチ ファイルが利用可能。
Prime Collaboration Provisioning	0.CSCur04871	脆弱性のあるリリースのパッチ ファイルが利用可能。
Unified Communication Audit Tool (UCAT)	0.CSCur05121	Affected systems have been patched.
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 シリーズ	0.CSCur04507	14.0.23（入手可能） 15.0.24（入手可能）
ASR1k、ASR903、ISR4400、CSR1000v 向け Cisco IOS XE	0.CSCur02734	15.4(2)S2/XE3.12.2S（入手可能） 15.4(3)S1/XE3.13.1S（入手可能） 15.5(1)S/XE3.14.0S（2015年11月30日） 15.4(1)S3/XE3.11.3S（2014年11月30日） 15.3(3)S5/XE3.10.5S（2015年1月31日） 15.2(4)S7/XE3.7.7S（2015年2月27日）
Catalyst 3k、4k、AIR-CT5760、お	0.CSCur03368	15.1(2)SG5/3.4.5SG（2014年11月

よび Cisco RF Gateway 10（RFGW-10）向け Cisco IOS XE		21日） 15.0(2)SG10/3.2.10SG（2014年12月31日） 15.2(1)E1/3.6.1E（2014年11月28日） 15.0(1)EZ5/3.3.5SE（入手可能）
Cisco MDS	0.CSCur01099	（脆弱性のあるリリースにはパッチファイルが用意されています）。
Cisco Nexus 1000仮想スーパーバイザモジュール(VSM)	0.CSCur04438	N1KV Vmware N1KV 5.2(1)SV3(1.2)（2014年11月中旬） N1KV HyperVリリース 5.2(1)SM2(1.1)（2014年12月1日）
Cisco Nexus 1010	0.CSCur04510	5.2(1)SP1(7.2)（入手可能）
Cisco Nexus 3000/3500	0.CSCur04934	6.0(2)U5(1)（入手可能） 6.0(2)U4(2)（入手可能） 6.0(2)U3(4)（入手可能） 6.0(2)U2(11Z)（入手可能）
Cisco Nexus 4000	0.CSCur05610	4.1(2)E1(1n)（2014年12月1日）
Cisco Nexus 5000/6000	0.CSCur05017	Gold Coast MR8 5.2(1)N1(8b)（入手可能） Harbord Plus MR4(a) 6.0(2)N2(5a)（入手可能） Iluka MR4 7.0(5)N1(1)（入手可能）
Cisco Nexus 7000 Series Switches	0.CSCur04856	5.2(9a)（入手可能） 6.1(5a)（入手可能） 6.2(8b)（入手可能） 6.2(10)（入手可能）
Cisco Nexus 7000	0.CSCuq98748	5.2(9a)（入手可能） 6.1(5a)（入手可能） 6.2(8b)（入手可能） 6.2(10)（入手可能）
Cisco Nexus 9000スイッチ	0.CSCur05011	6.1(2)I3(1)（入手可能）
NxOSを実行するCisco Nexus 9000	0.CSCur02700	6.1(2)I2(1)（入手可能） 6.1(2)I2(2)（入手可能） 6.1(2)I2(2a)（入手可能） 6.1(2)I2(2b)（入手可能） 6.1(2)I2(3)（入手可能） 6.1(2)I3(1)（入手可能）
Cisco Nexus 9000	0.CSCur02102	11.0(1d)（入手可能）
Cisco OnePK All-in-One VM	0.CSCur04925	（入手可能 – ベンダーのパッチを使用

		）
Cisco Quantum SON Suite（Cisco Quantum SON スイート）	0.CSCur05662	（影響を受けるシステムは、2015年2月1日までにパッチ適用を完了する予定）
Cisco Quantum Virtualized Packet Core	0.CSCur05662	（影響を受けるシステムは、2015年2月1日までにパッチ適用を完了する予定）
Cisco Service Control Engine 1010	0.CSCur05021	Cisco Service Control Engine 8000のパッチファイルは、2000年11月30日までに入手可能になる予定です。 パッチファイルは、2014年12月19日までにCisco Service Control Engine 10000で利用可能になる予定です。
Cisco Service Control Engine 8000	0.CSCur05021	Cisco Service Control Engine 8000のパッチファイルは、2000年11月30日までに入手可能になる予定です。 パッチファイルは、2014年12月19日までにCisco Service Control Engine 10000で利用可能になる予定です。
Cisco仮想スイッチアップデートマネージャ	0.CSCur12303	1.1 (Available)
Cisco Network Convergence System（NCS）6000 向け IOS-XR	0.CSCur02177	5.2.3（2014年12月31日） 5.0.1（SMUは2014年11月31日に利用可能） 5.2.1（SMUは2014年11月31日に利用可能）
ルーティングおよびスイッチング - スモール ビジネス		
Cisco WAG310G Residential Gateway	0.CSCur05525	アップグレードオプションについては、TACにお問い合わせください。
Unified Computing		
Cisco Standalone ラック サーバ CIMC	0.CSCur03816	1.4(3x/y)（2014年11月25日） 1.5(7d)（2014年11月25日） 2.0(3f/g)（2014年11月25日） 2.0(4x)（2014年11月25日） 2.0(2x)（2014年11月25日）
Cisco UCS Director	0.CSCur02877	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco UCS Invictaアプライアンス	0.CSCur05026	5.0.1.2（入手可能）
Cisco UCS Manager	0.CSCur01379	3.0(1d)（入手可能）

		2.2(3b)（入手可能） 2.2(2e)（入手可能） 2.2(1f)（入手可能） 2.1(3f)（入手可能） 2.0(5g)（入手可能）
Cisco USC Invictaシリーズ自動サポートポータル	0.CSCur07304	5.0.1.2（入手可能）
Cisco USC Invictaシリーズ	0.CSCur04651	5.0.1.2（入手可能）
Cisco Unified Computing System B-Series (Blade) Servers	0.CSCur05081	3.0.2（2015年2月15日）
Cisco Unified Computing System E シリーズ ブレード サーバ	0.CSCur05553	3.0.1（2015年7月提供開始）
Cisco Virtual Security Gateway	0.CSCur95323	5.2(1)VSG2(1.2c)（入手可能）
Cisco Virtualization Experience Client 6215	0.CSCur05844	（脆弱性のあるリリースにはパッチファイルが用意されています）。 10.6（15年1月22日）
音声およびユニファイド コミュニケーション デバイス		
Cisco Business Edition 3000(BE3k)	0.CSCur08462	アップグレードオプションについては、TACにお問い合わせください。
Cisco Emergency Responder	0.CSCur05434	パッチ：使用可能（以前のすべてのCERバージョン8.xに適用可能） 9.x 10.x)
Cisco Finesse	0.CSCur02866	脆弱性のあるリリースに対してパッチファイルを使用できます
Cisco Hosted Collaboration Mediation Fulfillment	0.CSCur05477	（該当するリリースにはパッチファイルが用意されています）。
Cisco IM and Presence Service（CUPS）	0.CSCur05454	（該当するリリースにはパッチファイルが用意されています）。 10.5.1 SU2（入手可能）
Cisco IP Interoperability and Collaboration System (IPICS)	0.CSCur05245	IPICS 4.8.2
Cisco MediaSense	0.CSCur02875	9.1 ES（入手可能） 10.5SU（パッチあり）：サポートされている任意のバージョンのMSで動作します。
Cisco Paging Server（Informacast）	0.CSCur04834	9.0.2（入手可能）

Cisco SocialMiner	0.CSCur02880	（該当するリリースにはパッチファイルが用意されています）。 10.6(1)（2014年12月17日）
Cisco Unified Communications Domain Manager	0.CSCur01180	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco Unified Communications Manager（CUCM）	0.CSCur00930	脆弱性のあるリリースのパッチ ファイルが利用可能。 10.5(1.11011.1)（入手可能） 10.0(1.13012.1)（入手可能） 9.1(2.13060.1)（入手可能） 8.6(2.26147.1)（入手可能） 8.5(1.17131.2)（入手可能）
Cisco Unified Contact Center Express（UCCX）	0.CSCur02861	脆弱性のあるリリースのパッチ ファイルが利用可能。 10.6(1)（2014年12月3日）
Cisco Unified Intelligence Center（CUIC）	0.CSCur02891	脆弱性のあるリリースのパッチ ファイルが利用可能。 CUIC 11.0(1)（2015年6月30日）
Cisco Unified Quick Connect	0.CSCur05412	アップグレードオプションについては、TACにお問い合わせください。
Cisco Unity Connection（UC）	0.CSCur05328	脆弱性のあるリリースのパッチ ファイルが利用可能。 8.6.2ES153（入手可能） 9.1.2ES67（入手可能） 10.5.1ES74（入手可能） 8.5.1（2014年12月中旬）
ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス		
Cisco AutoBackupサーバ	0.CSCur09315	Shellshock-1.0.1（すべてのDBDS Linux 5.x用） 6.x製品) – パッチが利用可能
Cisco D9036 Modular Encoding Platform	0.CSCur04504	v02.02.30（入手可能）
Cisco Digital Media Manager（DMM）	0.CSCur03539	5.3.1（入手可能） 5.3.7（入手可能） 5.3.10（入手可能） 5.3.11（入手可能） 5.3.12（入手可能） 5.5 (Available)
Cisco Digital Media	0.CSCur05628	5.3(6)RB(2P)（入手可能）

Player(DMP)4310		5.4(1)RB(2P)（入手可能）
Ciscoダウンロードサーバ(DLS)（RHベース）	0.CSCur09318	Shellshock-1.0.1（すべてのDBDS Linux 5.x用） 6.x製品) – パッチが利用可能
Cisco Edge 300 Digital Media Player	0.CSCur02761	脆弱性のあるリリースにはパッチ(V1.6.0)ファイルが用意されています。
Cisco Edge 340 Digital Media Player	0.CSCur02751	1.1.0.4 1.2（2014年12月20日）
Cisco Enterprise Content Deliveryサービス	0.CSCur02848	2.6.3（入手可能）
Cisco Media Experience Engine(MXE)	0.CSCur04893	3.3.2.（入手可能）
Cisco PowerVu D9190 Conditional Access Manager(PCAM)	0.CSCur05774	1.1（2015年4月30日に入手可能）
Cisco Show and Share（SnS）	0.CSCur03539	5.3.1（入手可能） 5.3.7（入手可能） 5.3.10（入手可能） 5.3.11（入手可能） 5.3.12（入手可能） 5.5 (Available)
Cisco StadiumVision Director	0.CSCur30139	StadiumVision:3.2 build 520(SP2)（入手可能）
Cisco StadiumVisionモバイルレポーター	0.CSCur30167	2.0.1（ビルド1）（入手可能）
Cisco StadiumVisionモバイルストリーマ	0.CSCur30155	2.0.1（ビルド1）（入手可能）
Cisco TelePresence 1310	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence Conductor	0.CSCur02103	XC2.4.1（入手可能） XC2.3.1（入手可能）
Cisco TelePresence Exchange System（CTX）	0.CSCur05335	1.3.0.4.2.0（2014年11月7日）
Cisco TelePresence ISDN Link	0.CSCur05025	1.1.4（入手可能）
Cisco TelePresence Manager（CTSMan）	0.CSCur05104	1.9.4（入手可能）
Cisco TelePresence Multipoint	0.CSCur05344	1.8.x（パッチファイルあり）

Switch (CTMS)		1.9.7（入手可能）
Cisco TelePresence Recording Server（CTRS）	0.CSCur05038	脆弱性のあるリリースで利用可能なパッチファイル。
Cisco TelePresence System 1000	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 1100	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 1300	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 3000 Series	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 500-32	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 500-37	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence TE Software (for E20 - EoL)	0.CSCur05162	4.1.5（入手可能）
Cisco TelePresence TX 9000 Series	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence Video Communication Server(VCS/Expressway)	0.CSCur01461	X8.2.2（入手可能） X7.2.4（使用可能） X8.1.2（使用可能）
Cisco TelePresenceエンドポイント（Cシリーズ、EXシリーズ、MXシリーズ、MXG2シリーズ、SXシリーズ）および10インチタッチパネル	0.CSCur02591	5.1.13（入手可能） 6.0.4（入手可能） 6.1.4（入手可能） 6.3.3（入手可能） 7.2.1（入手可能）
Cisco VDS Service Broker	0.CSCur05679	VDS-SB 1.4（2014年12月1日）
インターネットストリーミングVDS-IS向けCisco Video Distribution Suite	0.CSCur05320	3.3.1b112（入手可能） 4.0.0b157（入手可能） 4.1.0b036（2015年3月）

Cisco Video Surveillance Media Server	0.CSCur05423	（該当するリリースにはパッチファイルが用意されています）。 7.6.0（12月15日）
Cisco Virtual PGW 2200 ソフトスイッチ	0.CSCur05847	脆弱性のあるリリースのパッチ ファイルが利用可能。
シスコ ホステッド サービス		
シスコ クラウド サービス	0.CSCur05334	（該当するシステムにはパッチが適用されています）。
Cisco Common Services Platform Collector	0.CSCur07881	Affected systems have been patched.
Cisco Intelligent Automation for Cloud	0.CSCur05134	4.1.0.81287.195（入手可能）
シスコのライフサイクル管理(LCM)	0.CSCur05242	Affected systems have been patched.
Cisco NetAuthenticate（認証）	0.CSCur05632	Affected systems have been updated.
Cisco Proactive Network Operations Center	0.CSCur05856	（該当するシステムにはパッチが適用されています）。
Cisco Smart Care	0.CSCur05638	1.13.2.1（入手可能）
Cisco Universal Small Cell CloudBase	0.CSCur05647	（該当するシステムにはパッチが適用されています）。
Cisco WebEx ノード	0.CSCur10599	(Affected systems have been patched.
Network Performance Analytics (NPA)	0.CSCur05788	（該当するシステムにはパッチが適用されています）。
Web Element Manager	0.CSCur09009	（該当するシステムにはパッチが適用されています）。

製品	Defect	Fixed releases availability
ケーブル モデム		
Cisco Video Surveillance Media Server	0.CSCur05423	（該当するリリースにはパッチファイルが用意されています）。 7.6.0（12月15日）
ネットワーク アプリケーション、サービス、およびアクセラレーション		
Cisco Catalyst 6500用Cisco ACE Application Control Engineモジュール	0.CSCur02931	アップグレードオプションについては、TACにお問い合わせください。
Cisco Application Control Engine (ACE10 and ACE20)	0.CSCur07312	アップグレードオプションについては、TACにお問い合わせください。
Cisco Application Control	0.CSCur02195	（脆弱性のあるリリースに対してパッ

Engine（ACE30/ACE 4710）		チが提供されています）。 A5(3.1b)（11月30日、14日）
Cisco Application and Content Networking System（ACNS）	0.CSCur05564	5.5.37（12月14日）
Cisco DC Health Check	0.CSCur09963	DCAF 4.0（入手可能）
Cisco GSS 4492Rグローバルサイトセレクタ	0.CSCur02747	4.1(3.0.7)（入手可能） 3.2(0.1.4)（入手可能）
Cisco NAC アプライアンス	0.CSCur03364	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco Smart Call Home	0.CSCur05551	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco Visual Quality Experience Server	0.CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Visual Quality Experience Tools Server	0.CSCur06775	3.6 (Available) 3.7 (Available) 3.8 (Available) 3.9 (Available)
Cisco Wide Area Application Services（WAAS）	0.CSCur02917	パッチファイルは、4.4.xリリースと5.2.1bで使用できます。 5.0.3h（入手可能） 5.1.1h（入手可能） 5.3.5c（2014年11月25日）
ネットワークおよびコンテンツ セキュリティ デバイス		
Cisco ASA CX と Cisco Prime Security Manager	0.CSCur01959	9.3.2.1（入手可能）
Cisco Clean Access Manager	0.CSCur05566	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco FireSIGHT	0.CSCur05199	（脆弱性のあるリリースにはパッチファイルが用意されています）。 5.3.0.3（2014年11月30日） 5.3.1.1（入手可能） 5.2.0.7（入手可能） 4.10.3.10（入手可能）
Cisco Identity Services Engine（ISE）	0.CSCur00532	1.3.0.876（入手可能） 1.2.0パッチ12（入手可能） 1.2.1パッチ3（入手可能） 1.1.3パッチ12（12月14日）

		1.1.4パッチ12（12月14日）
シスコ侵入防御システム（IPS）	0.CSCur00552	7.1.9（入手可能） 7.3.3（2015年1月）
Cisco IronPort暗号化アプライアンス	0.CSCur02831	（脆弱性のあるリリースにはパッチファイルを使用できます）
Cisco NAC Guest Server	0.CSCur05629	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco NAC Server	0.CSCur05575	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco Physical Accessゲートウェイ	0.CSCur05343	1.5.3 (15-Apr-2015)
Cisco Physical Access Manager	0.CSCur05357	1.5.2（入手可能）
Cisco Secure Access Control Server（ACS）	0.CSCur00511	A patch is available for vulnerable releases.
Cisco Virtual Security Gateway for Microsoft Hyper-V	0.CSCur05042	5.2(1)VSG2(1.2a)（14年11月30日）
ネットワーク管理とプロビジョニング		
Cisco Access Registrarアプライアンス Cisco Prime Access Registrarアプライアンス	0.CSCur10557	5.x（入手可能） 6.x（入手可能）
Cisco Application Networking Manager	0.CSCur06823	5.2.5（入手可能）
Cisco MXEシリーズ	0.CSCur05088	3.3.2.（入手可能）
Cisco Media Experience Engines（MXE）	0.CSCur05088	3.3.2.（入手可能）
Cisco NetFlow Collection Agent	0.CSCur05232	脆弱性のあるリリースのパッチ ファイルが利用可能。 6.2（2015年6月1日から利用可能）
Cisco Network Analysis Module	0.CSCur05225	脆弱性のあるリリースのパッチ ファイルが利用可能。 6.2（2015年6月1日から利用可能）
Cisco Prime Collaboration Assurance	0.CSCur04820	10.5 (Available) 10.6（2014年12月15日）
Cisco Prime Collaboration Deployment	0.CSCur07766	A patch is available for vulnerable releases 10.5.2（2014年12月31日）
Cisco Prime IP Express	0.CSCur05200	8.2.0.5（2015年1月31日）
Cisco Prime Infrastructure	0.CSCur05228	A patch is available for vulnerable

		releases 2.1.2（使用可能）
Cisco Prime LAN Management Solution	0.CSCur05125	パッチによるLMS 4.2.5（2014年12月31日）
Cisco Prime License Manager	0.CSCur05098	10.5.1 SU（入手可能） 10.5.2（2014年12月31日）
Cisco Prime Network Registrar(CPNR)Jumpstart	0.CSCur05136	8.2.2.1（入手可能） 8.1.3.3（2015年1月31日） 7.2.3.5（2015年1月31日）
Cisco Prime Network Services Controller	0.CSCur05617	PNSC 3.4.1（入手可能）
Cisco Prime サービス カタログ仮想アプライアンス	0.CSCur10723	PSC 10.0-R2（入手可能）
Cisco UCS Central	0.CSCur05093	1.2(1d)（入手可能）
Data Center Analytics Framework（DCAF）	0.CSCur09685	4.0（利用可能）
デジタルメディアマネージャ(DMM)	0.CSCur03217	パッチは次のリリースで利用可能です。 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）	0.CSCur05780	2.2.6.1（入手可能） 2.2.7
ネットワーク構成と変更管理	0.CSCur05794	脆弱性のあるリリースのパッチ ファイルが利用可能。
Prime Collaboration Provisioning	0.CSCur04871	脆弱性のあるリリースのパッチ ファイルが利用可能。
Unified Communication Audit Tool (UCAT)	0.CSCur05121	Affected systems have been patched.
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 シリーズ	0.CSCur04507	14.0.23（入手可能） 15.0.24（入手可能）
ASR1k、ASR903、ISR4400、CSR1000v 向け Cisco IOS XE	0.CSCur02734	15.4(2)S2/XE3.12.2S（入手可能） 15.4(3)S1/XE3.13.1S（入手可能） 15.5(1)S/XE3.14.0S（2015年11月30日）

		15.4(1)S3/XE3.11.3S（2014年11月30日） 15.3(3)S5/XE3.10.5S（2015年1月31日） 15.2(4)S7/XE3.7.7S（2015年2月27日）
Catalyst 3k、4k、AIR-CT5760、および Cisco RF Gateway 10（RFGW-10）向け Cisco IOS XE	0.CSCur03368	15.1(2)SG5/3.4.5SG（2014年11月21日） 15.0(2)SG10/3.2.10SG（2014年12月31日） 15.2(1)E1/3.6.1E（2014年11月28日） 15.0(1)EZ5/3.3.5SE（入手可能）
Cisco MDS	0.CSCur01099	（脆弱性のあるリリースにはパッチファイルが用意されています）。
Cisco Nexus 1000仮想スーパーバイザモジュール(VSM)	0.CSCur04438	N1KV Vmware N1KV 5.2(1)SV3(1.2)（2014年11月中旬） N1KV HyperVリリース 5.2(1)SM2(1.1)（2014年12月1日）
Cisco Nexus 1010	0.CSCur04510	5.2(1)SP1(7.2)（入手可能）
Cisco Nexus 3000/3500	0.CSCur04934	6.0(2)U5(1)（入手可能） 6.0(2)U4(2)（入手可能） 6.0(2)U3(4)（入手可能） 6.0(2)U2(11Z)（入手可能）
Cisco Nexus 4000	0.CSCur05610	4.1(2)E1(1n)（2014年12月1日）
Cisco Nexus 5000/6000	0.CSCur05017	Gold Coast MR8 5.2(1)N1(8b)（入手可能） Harbord Plus MR4(a) 6.0(2)N2(5a)（入手可能） Iluka MR4 7.0(5)N1(1)（入手可能）
Cisco Nexus 7000 Series Switches	0.CSCur04856	5.2(9a)（入手可能） 6.1(5a)（入手可能） 6.2(8b)（入手可能） 6.2(10)（入手可能）
Cisco Nexus 7000	0.CSCuq98748	5.2(9a)（入手可能） 6.1(5a)（入手可能） 6.2(8b)（入手可能） 6.2(10)（入手可能）
Cisco Nexus 9000スイッチ	0.CSCur05011	6.1(2)I3(1)（入手可能）
NxOSを実行するCisco Nexus 9000	0.CSCur02700	6.1(2)I2(1)（入手可能）

		6.1(2)I2(2)（入手可能） 6.1(2)I2(2a)（入手可能） 6.1(2)I2(2b)（入手可能） 6.1(2)I2(3)（入手可能） 6.1(2)I3(1)（入手可能）
Cisco Nexus 9000	0.CSCur02102	11.0(1d)（入手可能）
Cisco OnePK All-in-One VM	0.CSCur04925	（入手可能 – ベンダーのパッチを使用）
Cisco Quantum SON Suite（Cisco Quantum SON スイート）	0.CSCur05662	（影響を受けるシステムは、2015年2月1日までにパッチ適用を完了する予定）
Cisco Quantum Virtualized Packet Core	0.CSCur05662	（影響を受けるシステムは、2015年2月1日までにパッチ適用を完了する予定）
Cisco Service Control Engine 1010	0.CSCur05021	Cisco Service Control Engine 8000のパッチファイルは、2000年11月30日までに入手可能になる予定です。 パッチファイルは、2014年12月19日までにCisco Service Control Engine 10000で利用可能になる予定です。
Cisco Service Control Engine 8000	0.CSCur05021	Cisco Service Control Engine 8000のパッチファイルは、2000年11月30日までに入手可能になる予定です。 パッチファイルは、2014年12月19日までにCisco Service Control Engine 10000で利用可能になる予定です。
Cisco仮想スイッチアップデートマネージャ	0.CSCur12303	1.1 (Available)
Cisco Network Convergence System（NCS）6000 向け IOS-XR	0.CSCur02177	5.2.3（2014年12月31日） 5.0.1（SMUは2014年11月31日に利用可能） 5.2.1（SMUは2014年11月31日に利用可能）
ルーティングおよびスイッチング - スモール ビジネス		
Cisco WAG310G Residential Gateway	0.CSCur05525	アップグレードオプションについては、TACにお問い合わせください。
Unified Computing		
Cisco Standalone ラック サーバ CIMC	0.CSCur03816	1.4(3x/y)（2014年11月25日） 1.5(7d)（2014年11月25日）

		2.0(3f/g)（2014年11月25日） 2.0(4x)（2014年11月25日） 2.0(2x)（2014年11月25日）
Cisco UCS Director	0.CSCur02877	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco UCS Invictaアプライアンス	0.CSCur05026	5.0.1.2（入手可能）
Cisco UCS Manager	0.CSCur01379	3.0(1d)（入手可能） 2.2(3b)（入手可能） 2.2(2e)（入手可能） 2.2(1f)（入手可能） 2.1(3f)（入手可能） 2.0(5g)（入手可能）
Cisco USC Invictaシリーズ自動サポートポータル	0.CSCur07304	5.0.1.2（入手可能）
Cisco USC Invictaシリーズ	0.CSCur04651	5.0.1.2（入手可能）
Cisco Unified Computing System B-Series (Blade) Servers	0.CSCur05081	3.0.2（2015年2月15日）
Cisco Unified Computing System E シリーズ ブレード サーバ	0.CSCur05553	3.0.1（2015年7月提供開始）
Cisco Virtual Security Gateway	0.CSCur95323	5.2(1)VSG2(1.2c)（入手可能）
Cisco Virtualization Experience Client 6215	0.CSCur05844	（脆弱性のあるリリースにはパッチファイルが用意されています）。 10.6（15年1月22日）
音声およびユニファイド コミュニケーション デバイス		
Cisco Business Edition 3000(BE3k)	0.CSCur08462	アップグレードオプションについては、TACにお問い合わせください。
Cisco Emergency Responder	0.CSCur05434	パッチ：使用可能（以前のすべてのCERバージョン8.xに適用可能） 9.x 10.x)
Cisco Finesse	0.CSCur02866	脆弱性のあるリリースに対してパッチファイルを使用できます
Cisco Hosted Collaboration Mediation Fulfillment	0.CSCur05477	（該当するリリースにはパッチファイルが用意されています）。
Cisco IM and Presence Service（CUPS）	0.CSCur05454	（該当するリリースにはパッチファイルが用意されています）。 10.5.1 SU2（入手可能）
Cisco IP Interoperability and	0.CSCur05245	IPICS 4.8.2

Collaboration System (IPICS)		
Cisco MediaSense	0.CSCur02875	9.1 ES（入手可能） 10.5SU（パッチあり）：サポートされている任意のバージョンのMSで動作します。
Cisco Paging Server（Informacast）	0.CSCur04834	9.0.2（入手可能）
Cisco SocialMiner	0.CSCur02880	（該当するリリースにはパッチファイルが用意されています）。 10.6(1)（2014年12月17日）
Cisco Unified Communications Domain Manager	0.CSCur01180	脆弱性のあるリリースのパッチ ファイルが利用可能。
Cisco Unified Communications Manager（CUCM）	0.CSCur00930	脆弱性のあるリリースのパッチ ファイルが利用可能。 10.5(1.11011.1)（入手可能） 10.0(1.13012.1)（入手可能） 9.1(2.13060.1)（入手可能） 8.6(2.26147.1)（入手可能） 8.5(1.17131.2)（入手可能）
Cisco Unified Contact Center Express（UCCX）	0.CSCur02861	脆弱性のあるリリースのパッチ ファイルが利用可能。 10.6(1)（2014年12月3日）
Cisco Unified Intelligence Center（CUIC）	0.CSCur02891	脆弱性のあるリリースのパッチ ファイルが利用可能。 CUIC 11.0(1)（2015年6月30日）
Cisco Unified Quick Connect	0.CSCur05412	アップグレードオプションについては、TACにお問い合わせください。
Cisco Unity Connection（UC）	0.CSCur05328	脆弱性のあるリリースのパッチ ファイルが利用可能。 8.6.2ES153（入手可能） 9.1.2ES67（入手可能） 10.5.1ES74（入手可能） 8.5.1（2014年12月中旬）
ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス		
Cisco AutoBackupサーバ	0.CSCur09315	Shellshock-1.0.1（すべてのDBDS Linux 5.x用） 6.x製品) – パッチが利用可能
Cisco D9036 Modular Encoding Platform	0.CSCur04504	v02.02.30（入手可能）

Cisco Digital Media Manager（DMM）	0.CSCur03539	5.3.1（入手可能） 5.3.7（入手可能） 5.3.10（入手可能） 5.3.11（入手可能） 5.3.12（入手可能） 5.5 (Available)
Cisco Digital Media Player(DMP)4310	0.CSCur05628	5.3(6)RB(2P)（入手可能） 5.4(1)RB(2P)（入手可能）
Ciscoダウンロードサーバ(DLS)（RHベース）	0.CSCur09318	Shellshock-1.0.1（すべてのDBDS Linux 5.x用） 6.x製品) – パッチが利用可能
Cisco Edge 300 Digital Media Player	0.CSCur02761	脆弱性のあるリリースにはパッチ(V1.6.0)ファイルが用意されています。
Cisco Edge 340 Digital Media Player	0.CSCur02751	1.1.0.4 1.2（2014年12月20日）
Cisco Enterprise Content Deliveryサービス	0.CSCur02848	2.6.3（入手可能）
Cisco Media Experience Engine(MXE)	0.CSCur04893	3.3.2.（入手可能）
Cisco PowerVu D9190 Conditional Access Manager(PCAM)	0.CSCur05774	1.1（2015年4月30日に入手可能）
Cisco Show and Share（SnS）	0.CSCur03539	5.3.1（入手可能） 5.3.7（入手可能） 5.3.10（入手可能） 5.3.11（入手可能） 5.3.12（入手可能） 5.5 (Available)
Cisco StadiumVision Director	0.CSCur30139	StadiumVision:3.2 build 520(SP2)（入手可能）
Cisco StadiumVisionモバイルレポーター	0.CSCur30167	2.0.1（ビルド1）（入手可能）
Cisco StadiumVisionモバイルストリーマ	0.CSCur30155	2.0.1（ビルド1）（入手可能）
Cisco TelePresence 1310	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence Conductor	0.CSCur02103	XC2.4.1（入手可能） XC2.3.1（入手可能）

Cisco TelePresence Exchange System（CTX）	0.CSCur05335	1.3.0.4.2.0（2014年11月7日）
Cisco TelePresence ISDN Link	0.CSCur05025	1.1.4（入手可能）
Cisco TelePresence Manager（CTSMan）	0.CSCur05104	1.9.4（入手可能）
Cisco TelePresence Multipoint Switch (CTMS)	0.CSCur05344	1.8.x（パッチファイルあり） 1.9.7（入手可能）
Cisco TelePresence Recording Server（CTRS）	0.CSCur05038	脆弱性のあるリリースで利用可能なパッチファイル。
Cisco TelePresence System 1000	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 1100	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 1300	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 3000 Series	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 500-32	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence System 500-37	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence TE Software (for E20 - EoL)	0.CSCur05162	4.1.5（入手可能）
Cisco TelePresence TX 9000 Series	0.CSCur05163	1.9.8（入手可能） 6.1.5.1（入手可能） 1.10.8.1（入手可能）
Cisco TelePresence Video Communication Server(VCS/Expressway)	0.CSCur01461	X8.2.2（入手可能） X7.2.4（使用可能） X8.1.2（使用可能）
Cisco TelePresenceエンドポイント（Cシリーズ、EXシリーズ、MXシリーズ、MXG2シリーズ、SXシリ	0.CSCur02591	5.1.13（入手可能） 6.0.4（入手可能） 6.1.4（入手可能）

ーズ）および10インチタッチパネル		6.3.3（入手可能） 7.2.1（入手可能）
Cisco VDS Service Broker	0.CSCur05679	VDS-SB 1.4（2014年12月1日）
インターネットストリーミング VDS-IS向けCisco Video Distribution Suite	0.CSCur05320	3.3.1b112（入手可能） 4.0.0b157（入手可能） 4.1.0b036（2015年3月）
Cisco Virtual PGW 2200 ソフトスイッチ	0.CSCur05847	脆弱性のあるリリースのパッチ ファイルが利用可能。
シスコ ホステッド サービス		
シスコ クラウド サービス	0.CSCur05334	（該当するシステムにはパッチが適用されています）。
Cisco Common Services Platform Collector	0.CSCur07881	Affected systems have been patched.
Cisco Intelligent Automation for Cloud	0.CSCur05134	4.1.0.81287.195（入手可能）
シスコのライフサイクル管理(LCM)	0.CSCur05242	Affected systems have been patched.
Cisco NetAuthenticate（認証）	0.CSCur05632	Affected systems have been updated.
Cisco Proactive Network Operations Center	0.CSCur05856	（該当するシステムにはパッチが適用されています）。
Cisco Smart Care	0.CSCur05638	1.13.2.1（入手可能）
Cisco Universal Small Cell CloudBase	0.CSCur05647	（該当するシステムにはパッチが適用されています）。
Cisco WebEx ノード	0.CSCur10599	(Affected systems have been patched.
Network Performance Analytics (NPA)	0.CSCur05788	（該当するシステムにはパッチが適用されています）。
Web Element Manager	0.CSCur09009	（該当するシステムにはパッチが適用されています）。

脆弱性を含んでいないことが確認された製品

注：次のリストには、お客様が用意したホスト（物理サーバまたは仮想マシン）に、お客様がインストールしたオペレーティングシステムとともにインストールすることを目的としたシスコのアプリケーションが含まれています。これらの製品では、シスコ製品がインストールされているホストオペレーティングシステムで提供されるBashシェルを使用できます。これらのシスコ製品には該当バージョンのBashが直接含まれていないため、この脆弱性の影響を受けることはありませんが、オペレーティングシステムのベンダーの推奨事項と一般的なオペレーティングシステムセキュリティのベストプラクティスに従って、ホストオペレーティングシステムのインストールを確認し、この脆弱性に対処するために必要なアップグレードを実行することをお勧めします。

次のシスコ製品は分析済みであり、この脆弱性の影響を受けません。

ケーブル モデム

- Cisco Prime Network Registrar（CPNR）
- Digital Life RMSおよび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

エンドポイント クライアントとクライアント ソフトウェア

- 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

ネットワーク アプリケーション、サービス、およびアクセラレーション

- Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Cisco Extensible Network Controller（XNC）
- Cisco Firewall Services モジュール
- Cisco Nexus Data Broker Cisco Extensible Network Controller(XNC)
- Cisco Openflowエージェント
- コンテンツ サービス スイッチ

ネットワークおよびコンテンツ セキュリティ デバイス

- 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 セキュリティ管理アプライアンス（SMA）

ネットワーク管理とプロビジョニング

- 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ネットワークコレクタ
- Cisco Prime Access Registrar
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Data Centerネットワークマネージャ
- Cisco Prime Home
- Cisco Prime Network
- Cisco Prime Optical for SPs
- SP向けCisco Prime Performance Manager
- Cisco Quantum Policy Suite (QPS)
- Cisco Security Manager
- Cisco TelePresence MPS Series
- Cisco Unified Provisioning Manager（CUPM）
- CiscoWorks Network Compliance Manager
- ネットワークプロファイラ
- Security Module for Cisco Network Registrar
- ユニファイド コミュニケーション導入ツール

Routing and Switching - Enterprise and Service Provider

- CRS-CGSE-PLIM CRS-CGSE-PLUS
- Cisco 1000 シリーズ Connected Grid ルータ
- Cisco ASR 9000 シリーズ統合型サービス モジュール
- Cisco Application Policy Infrastructure Controller
- Cisco Broadband Access Center Telco Wireless
- Cisco Connected Grid Device Manager
- Cisco Connected Gridルータ(CGR)

- Cisco IOS
- Cisco IOS-XRの実行

    - Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ
    - Cisco CRSルータ
    - Cisco XR 12000 シリーズ ルータ
- Cisco Metro Ethernet 1200 シリーズ アクセス デバイス
- 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

ルーティングおよびスイッチング - スモール ビジネス

- Cisco RV180W Wireless-N Multifunction VPN Router
- Cisco Small Business AP500 シリーズ ワイヤレス アクセス ポイント
- Cisco Small Business ISA500 Series Integrated Security Appliances
- Cisco Small Business RV 120W Wireless-N VPNファイアウォール
- Cisco Small Business RV シリーズ ルータ 0xxv3
- Cisco Small Business RV シリーズ ルータ RV110W
- Cisco Small Business RV シリーズ ルータ RV130x
- Cisco Small Business RV シリーズ ルータ RV215W
- Cisco Small Business RV シリーズ ルータ RV220W
- Cisco Small Business RV シリーズ ルータ RV315W
- Cisco Small Business RV シリーズ ルータ RV320
- Cisco Sx220 switches
- Cisco WAP4410N Wireless-N Access Point

Unified Computing

- Cisco Common Services Platform Collector
- Cisco Intercloudファブリック
- Cisco UCSシリーズファブリックエクステンダI/Oモジュール

音声およびユニファイド コミュニケーション デバイス

- 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 および DX80
- Cisco H.323 Signaling Interface
- Cisco IP Phone 8800 Series
- Cisco Jabber for Windows
- Cisco MS200X Ethernet Access Switch
- Cisco PGW 2200 ソフトスイッチ
- 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回線IP電話
- Cisco SPA8000 8 ポート IP テレフォニー ゲートウェイ
- Cisco SPA8800 IP テレフォニー ゲートウェイ（4 FXS ポートと 4 FXO ポートを内蔵）
- Cisco Sx300 switches
- Cisco Sx500スイッチ
- Cisco TAPI Service Provider（TSP）
- Cisco Unified 3900 シリーズ IP フォン
- Cisco Unified 6900 Series IP Phones
- Cisco Unified 6911 IP フォン
- Cisco Unified 6945 IP フォン
- Cisco Unified 7800 Series IP Phones
- Cisco Unified 8961 IP フォン
- Cisco Unified 9951 IP フォン
- Cisco Unified 9971 IP フォン
- 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サイジングツール
- Cisco Unified CommunicationsウィジェットClick To Call
- Cisco Unified Contact Center Enterprise

- Cisco Unified E-Mail Interaction Manager
- Cisco Unified IP 会議用電話 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
- Cisco Virtualization Experience Media Engine
- xony VIM/CCDM/CCMP

ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス

- Cisco AnyRes Live（CAL）
- Cisco AnyRes VOD(CAV)
- Cisco Command 2000 Server（cmd2k）（RH ベース）
- 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シリーズ990x-Digital Content Manager
- Cisco DNCS Application Server（AppServer）
- Cisco Digital Network Control System(DNCS)
- Cisco Digital Transport Adapter Control System（DTACS）
- Ciscoダウンロードサーバ(DLS)
- Cisco Explorer Control Suite(ECS)
- Cisco Explorerコントローラ(EC)
- Cisco IPTV Services Delivery System（ISDS）

- シスコ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リモートネットワークコントロールシステム(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バックオフィス(VBO)
- Cisco Videoscape Conductor
- Cisco Videoscape Distribution Suite Transparent Caching
- Cloud Object Store（COS）
- D9859 Advanced Receiverトランスコーダ

- Digital Media Player(DMP)4400 Digital Media Player(DMP)4310
- メディアサービスインターフェイス
- Tandberg Codian ISDN GW 3210/3220/3240
- Tandberg Codian MSE 8320 model
- VDS-Recorder
- VDS-TV Caching GW
- VDS-TV Streamer
- VDS-TV Vault

ワイヤレス

- Cisco IOSを実行しているCisco Aironetアクセスポイント
- Cisco Merakiクラウドマネージド屋内アクセスポイント
- Cisco Merakiクラウドマネージド屋外アクセスポイント
- Cisco Meraki MSアクセススイッチ
- 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)

シスコ ホステッド サービス

- ビジネス ビデオ サービス自動化ソフトウェア（BV）
- Cisco クラウド E メール セキュリティ
- シスコのクラウドおよびシステム管理
- Cisco Connected Analytics For Collaboration
- Cisco Connected Analytics for Network Deployment(CAND)
- Cisco Install Base Management(IBM)
- Cisco Oneビュー
- Cisco Registered Envelope Service（CRES）
- シスコのスリム
- Cisco Serial Number Assessment Service(SNAS)
- MSA向けシスコサービスプロビジョニングプラットフォーム(SPP)
- Cisco Smart Net Total Care(SNTC)
- Cisco Unified Services Delivery Platform（CUSDP）
- Cisco Universal Small Cell 5000シリーズ
- Cisco Universal Small Cell 7000シリーズ
- Cisco WebExミーティングクライアントと生産性ツール
- Cisco WebEx Messenger Service
- Cisco WebEx WebOffice および Workspace

- ICキャプチャ
- IMS
- パートナーサポートサービス(PSS)1.x
- Partner Support ServiceのSIコンポーネント
- スモールセルファクトリリカバリ
- Smart Net Total Care
- WebEx接続
- WebEx Event Center、Meeting Center、Training Center、およびSales Center
- WebEx PCNow
- WebExクイックブック
- WebEx11アプリケーションサーバ

詳細

bashシェルでは、シェル変数と関数をプロセス環境を通じて親から子にエクスポートできます。関数の定義は、関数の名前を共有し、`() {`で始まる環境変数を使用して渡されます。

子bashプロセスは、関数定義で渡される閉じカッコ`}`の処理後も、コードの処理と実行を停止しません。攻撃者は、`FUNCT=() { ignored; }; /bin/id`などの関数変数を定義して、環境が子プロセスにインポートされたときに /bin/idを実行する可能性があります。

SSHなどの一部の攻撃ベクトルを悪用するには認証に成功する必要があり、その結果ユーザに追加の特権が付与されることはないため、この脆弱性がシスコ製品に与える影響は製品によって異なる場合があります。

この脆弱性に対してCommon Vulnerabilities and Exposures(CVE)IDとしてCVE-2014-6271、CVE-2014-7169、CVE-2014-7186、CVE-2014-7187、CVE-2014-62 78.

管理者がプラットフォームで実行されているBashのバージョンが修正されているかどうかを確認するために、いくつかのソフトウェアツールが作成されています。これらのツールのいくつかは、誤検出の結果を提供したり、Bashシェルをクラッシュさせたりします。 Cisco Bug Search Toolで各バグIDに提供される情報は、修正コードが含まれているソフトウェアのバージョンを特定するもので、製品に脆弱性があるかどうかを判断するために使用する必要があります。

回避策

影響を受けるシステムで直接実行できるこの脆弱性に対する緩和策はありません。ただし、一部のお客様では、次のネットワークベースの緩和策が役に立つ場合があります。

- Cisco Intrusion Protection System(IPS)シグニチャ4689-0が作成され、リリースS824で使用可能になりました
- Cisco Sourcefireは、Bashの脆弱性からネットワークを検出して保護するために、31975-

31977、31985、32038-32039、32041-32043、32045-32047、および32049のSnortシグニチャを公開しています

シスコはこの脆弱性に対するEvent Responseを公開しています。
http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Bash_09252014.html

ネットワーク内のシスコデバイスに適用可能な対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=35836

修正済みソフトウェア

シスコは、脆弱性のある製品のソフトウェアアップグレードを提供する予定です。修正を含むソフトウェアバージョンなど、修正に関する情報は、脆弱な製品のリストからCisco Bug IDを参照し、Cisco Bug Search Toolで入力することで参照できます。

ソフトウェアのアップグレードを検討する場合は、バグのリリースノートとhttp://www.cisco.com/go/psirtのCisco Security Advisories, Responses, and Noticesアーカイブを参照し、後続のアドバイザリを参照して侵害の可能性と完全なアップグレードソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性はStephane Chazelas氏によって報告され、2014年9月24日にGNU Foundationによってリリースされました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash

改訂履歴

リビジョン 1.29	2015 年 4 月 1 日	「修正済みソフトウェア」の表と「脆弱性を含んでいないこと

		が確認された製品」のセクションを更新。
リビジョン 1.28	2015年3月2日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.27	2015年1月12日	修正済みソフトウェアの表を更新。
リビジョン 1.26	2014年12月5日	修正済みソフトウェアの表を更新。
リビジョン 1.25	2014-November-24	修正済みソフトウェアの表を更新。
リビジョン 1.24	2014-November-22	修正済みソフトウェアの表を更新。
リビジョン 1.23	2014-November-20	修正済みソフトウェアの表を更新。
リビジョン 1.22	2014-November-18	修正済みソフトウェアの表を更新。
リビジョン 1.21	2014-November-13	修正済みソフトウェアの表を更新。
リビジョン 1.20	2014-November-12	修正済みソフトウェアの表を更新。
リビジョン 1.19	2014年11月10日	修正済みソフトウェアの表を更新。
リビジョン 1.18	2014年11月7日	修正済みソフトウェアの表を更新。
リビジョン 1.17	2014年11月6日	修正済みソフトウェアの表を更新。
リビジョン 1.16	2014年11月5日	修正済みソフトウェアの表を更新。
リビジョ	2014年11月	修正済みソフトウェアの表を更

ン 1.15	4日	新。
リビジョン 1.14	2014年11月3日	修正済みソフトウェアの表を追加。
リビジョン 1.13	2014年10月22日	「脆弱性を含んでいないことが確認された製品」セクションを更新。
リビジョン 1.12	2014年10月15日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.11	2014年10月10日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.10	2014年10月9日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
Revision 1.9	2014年10月8日	修正情報の参照先の詳細、テストツールの詳細、「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.8	2014年10月6日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
Revision 1.7	2014年10月3日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
Revision 1.6	2014年10月2日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
Revision 1.5	2014年10月1日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んで

		いないことが確認された製品」のセクションを更新。
リビジョン 1.4	2014年9月30日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.3	2014年9月29日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.2	2014年9月27日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.1	2014年9月26日	「該当製品」、「脆弱性が存在する製品」、「脆弱性を含んでいないことが確認された製品」のセクションを更新。
リビジョン 1.0	2014年9月26日	初回公開リリース

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。