

シスコ製品に影響するGNU glibcの脆弱性 : 2016年2月



アドバイザリーID : cisco-sa-20160218-

[CVE-2015-](#)

glibc

[7547](#)

初公開日 : 2016-02-18 20:22

最終更新日 : 2017-02-13 18:20

バージョン 1.17 : Final

回避策 : No workarounds available

Cisco バグ ID : [CSCuy47726](#) [CSCuy74706](#)

[CSCuy36572](#) [CSCuy36594](#) [CSCuy35261](#)

[CSCuy35262](#) [CSCuy36433](#) [CSCuy35268](#)

[CSCuy36412](#) [CSCuy36610](#) [CSCuy35265](#)

[CSCuy36531](#) [CSCuy36597](#) [CSCuy36613](#)

[CSCuy35269](#) [CSCuy36413](#) [CSCuy74701](#)

[CSCuy34875](#) [CSCuy36513](#) [CSCuy36612](#)

[CSCuy74702](#) [CSCuy36606](#) [CSCuy38927](#)

[CSCuy36549](#) [CSCuy51595](#) [CSCuy35251](#)

[CSCuy32284](#) [CSCuy36620](#) [CSCuy36566](#)

[CSCuy35276](#) [CSCuy36443](#) [CSCuy36564](#)

[CSCuy74698](#) [CSCuy36547](#) [CSCuy36602](#)

[CSCuy38924](#) [CSCuy36427](#) [CSCuy36548](#)

[CSCuy36603](#) [CSCuy34700](#) [CSCuy36546](#)

[CSCuy36568](#) [CSCuy38921](#) [CSCuy38943](#)

[CSCuy36539](#) [CSCuy36619](#) [CSCuy37090](#)

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

2016年2月16日、GNU Cライブラリ(glibc)の業界全体にわたる重大な脆弱性が公開されました。

複数のシスコ製品に、脆弱性の影響を受ける可能性のある glibcのバージョンが組み込まれています。この脆弱性により、認証されていないリモートの攻撃者がバッファオーバーフロー状態を引き起こして、サービス拒否(DoS)状態を引き起こしたり、該当デバイスで任意のコードを実行したりする可能性があります。

シスコでは、この脆弱性に対処するソフトウェア アップデートをリリースする予定です。

この脆弱性に対処する回避策はありません。

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-20160218-glibc>

該当製品

シスコでは、本脆弱性の影響を受ける製品と影響の範囲を特定するために、製品ラインを調査しました。製品が該当するかどうかについては、このアドバイザリの「脆弱性が存在する製品」および「脆弱性を含んでいないことが確認された製品」のセクションを参照してください。

「脆弱性が存在する製品」セクションに、影響を受ける各製品のCisco Bug IDを示します。バグは [Cisco Bug Search Tool](#) で検索でき、回避策（利用可能な場合）や修正されたソフトウェアバージョンなど、プラットフォーム固有の追加情報が含まれています。

脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示し、修正済みソフトウェアの対象リリース日およびバージョンに関するガイダンスを提供します。

特定の修正済みソフトウェアバージョンに関する詳細情報は、このアドバイザリの「脆弱性のある製品」の表に記載されているCisco Bugsに記載されます。Bugs は、 [Cisco Bug Search Tool](#) で検索できます。ソフトウェアのアップグレードを計画する際は、バグを直接確認してください。バグには最新の情報が含まれています。

重要：Cisco Nexusスイッチがこの脆弱性の影響を受けるかどうかについては、表の最後にスイッチ名の横に表示されている参照記号の対応する脚注を参照してください。

製品	Cisco Bug ID	Fixed Release
Collaboration and Social Media		
Cisco SocialMiner	0.CSCuy74702	
Cisco WebEx Meetings Server versions 1.x	0.CSCuy36539	2.0.1.956 (2016年3月31日) パッチは https://software.cisco.com/download/release.html?i=ly&mdfio からダウンロードできます。
Cisco WebEx Meetings Server versions 2.x	0.CSCuy36539	2.0.1.956 (2016年3月31日) パッチは https://software.cisco.com/download/release.html?i=ly&mdfio からダウンロードできます。

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 Jabber Guest 10.0(2)	0.CSCuy36613	10.6(11) (2016年5月30日)
Cisco MMP サーバ	0.CSCuy36542	Affected systems have been updated.
ネットワーク アプリケーション、サービス、およびアプリケーション		
Cisco Intercloud フォールトトレランス	0.CSCuy36549	お客様は、Redhat経由でアップグレードして、この脆弱性を修正する必要があります。
Cisco Prime Network Service Controller(PNSC)	0.CSCuy36549	お客様は、Redhat経由でアップグレードして、この脆弱性を修正する必要があります。
Cisco Visual Quality Experience Server	0.CSCuy35276	影響を受けるシステムがアップグレードされました
Cisco Visual Quality Experience Tools Server	0.CSCuy35276	影響を受けるシステムがアップグレードされました
ネットワークおよびコンテンツ セキュリティ		
Cisco FireSIGHT IPSセンサー	0.CSCuy32284	5.4.0.7/5.4.1.6 DC (2016年3月21日) 5.4.1.6ケントン (2016年3月21日) 5.3.0./5.3.1.7 (2016年3月28日)
Cisco FireSIGHT システム ソフトウェア	0.CSCuy32284	5.4.0.7/5.4.1.6 DC (2016年3月21日) 5.4.1.6ケントン (2016年3月21日) 5.3.0./5.3.1.7 (2016年3月28日)
Cisco Identity Services Engine (ISE)	0.CSCuy34700	2.0 P3 (2016年4月)
Cisco Physical Access Manager	0.CSCuy35286	影響を受けるバージョンは更新されます (2016年4月15日)
Cisco Secure ACS 5.x	0.CSCuy36585	5.7パッチ2 (2016年3月11日) 5.8 patch2 (2016年4月)
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	0.CSCuy36565	7.1 (2016年4月15日)
Cisco Application Policy Infrastructure Controller エンタープライズモジュール (APICEM)	0.CSCuy37090	1.1 (March 2016)
Cisco Policy	0.CSCuy51595	9.1 (April 2016)

Suite(CPS)		
Cisco Prime Access Registrar アプライアンス	0.CSCuy36565	7.1 (2016年4月15日)
Cisco Prime Analytics	0.CSCuy36447	Redhat 6.5 for OSにアップグレードしてください。
Cisco Prime Central for SPs	0.CSCuy36443	1.5.1 (2016年3月30日)
Cisco Prime Collaboration Deployment	0.CSCuy36602	11.5.2 (July 2016)
Cisco Prime Data Center Network Manager (.ova および .iso インストーラ)	0.CSCuy36546	8.0(1) (April 2016)
Cisco Prime IP Express	0.CSCuy36566	お客様は、RedHat yumユーティリティを使用して、該当パッケージのアップグレード後にデバイスを再起動する必要があります。
Cisco Prime License Manager	0.CSCuy35265	11.5 (June 2016)
Cisco Prime Network Registrar (CPNR) 仮想アプライアンス	0.CSCuy36564	Affected systems have been updated.
Cisco Prime Network Registrar IP アドレス マネージャ (IPAM)	0.CSCuy36427	8.3 (2016年11月30日)
Cisco Prime Optical for SPs	0.CSCuy36433	10.006 (2016年7月31日)
Cisco Prime サービス カタログ仮想アプライアンス	0.CSCuy34875	お客様は、RedHat yumユーティリティを使用して、該当パッケージのアップグレード後にデバイスを再起動する必要があります。
Cisco Unified Intelligence Center	0.CSCuy74698	
Cisco Videoscape Distribution Suite サービス マネージャ	0.CSCuy35261	Affected systems have been updated.
Routing and Switching - Enterprise and Service		
Cisco ASR 5000 シリーズ	0.CSCuy36531	18.6.0 (2016年3月18日) 19.4.0 (2016年6月30日) 20.0.0 (2016年3月31日)

		<p>release/notes/70322a_patch_nxos_rn.html</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322a_patch_nxos_rn.html</p> <p>release/notes/70322b_patch_nxos_rn.html</p>
Cisco Nexus 3172シリーズスイッチ*2	0.CSCuy38921	<p>パッチは次のサイトで入手可能です。</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322a_patch_nxos_rn.html</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322b_patch_nxos_rn.html</p>
Cisco Nexus 3232Cスイッチ*1	0.CSCuy36553	<p>パッチは次のサイトで入手できます。</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322a_patch_nxos_rn.html</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322b_patch_nxos_rn.html</p>
Cisco Nexus 3264Qスイッチ*1	0.CSCuy36553	<p>パッチは次のサイトで入手できます。</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322a_patch_nxos_rn.html</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322b_patch_nxos_rn.html</p>
Cisco Nexus 9000 (ACI/Fabric Switch)	0.CSCuy37040	11.2(3x) (2016年4月)
Cisco Nexus 9000シリーズスイッチ (スタンドアロン、NxOSを実行) *1	0.CSCuy36553	<p>パッチは次のサイトで入手できます。</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322a_patch_nxos_rn.html</p> <p>http://www.cisco.com/c/en/us/td/docs/switches/datacenter/next-generation/switches/nexus/switches/70322b_patch_nxos_rn.html</p>
Cisco Prime Data Centerネットワークマネージャ	0.CSCuy36547	1.2(3x) (2016年5月)
IOS-XE 16.2.x	0.CSCuy38943	<p>16.1.3 (2016年5月31日)</p> <p>16.2 (2016年3月31日)</p>
Unified Computing		
Cisco UCS ADA	0.CSCuy35223	Affected systems have been updated.
Cisco UCS Director	0.CSCuy36413	該当するシステムはアップデート済み (2016年3月31日)
Cisco UCS Invicta シリーズ	0.CSCuy36550	<p>アプライアンス5.0.1.2d (2016年4月30日)</p> <p>スケール5.0.1.3c (2016年5月30日)</p>
音声およびユニファイド コミュニケーション		
Cisco 8800 シリーズ IPフォン	0.CSCuy47726	11.5(0) (March 31 2016) 。

Cisco Emergency Responder	0.CSCuy36606	11.5 (June 2016)
Cisco Finesse	0.CSCuy74706	
Cisco Hosted Collaboration Mediation Fulfillment	0.CSCuy36610	
Cisco IM and Presence Service (CUPS)	0.CSCuy36608	Affected systems have been updated.
Cisco MediaSense	0.CSCuy36619	11.5.1 (2016年3月31日) 11.0.1 (2016年3月31日)
Cisco Paging Server (Informacast)	0.CSCuy36612	11.5.1 (June 2016)
Cisco Paging Server	0.CSCuy36612	11.5.1 (June 2016)
Cisco Unified 7800 Series IP Phones	0.CSCuy36620	11.5(1) (April 2016)
Cisco Unified Communications Domain Manager	0.CSCuy36513	8.1.8 (July 2016)
Cisco Unified Communications Manager (UCM)	0.CSCuy32014	
Cisco Unified Communications Manager Session Management Edition (SME)	0.CSCuy32014	
Cisco Unified Contact Center Express - Live Data Server	0.CSCuy74701	
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	0.CSCuy36600	
Cisco Unity Connection (UC)	0.CSCuy36603	11.5 (2016年3月3日)
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		
Cisco DCM Series	0.CSCuy35251	

9900-Digital Content Manager		
Cisco Edge 300 Digital Media Player	0.CSCuy35298	1.6RB4_5(18-Mar-2016)
Cisco Edge 340 Digital Media Player	0.CSCuy35299	1.2.0.19 (2016年3月31日)
Cisco Expressway Series	0.CSCuy35269	X8.7.2 (2016年3月31日)
Cisco Powerkey Encryption Server (PKES)	0.CSCuy37232	
Cisco TelePresence Conductor	0.CSCuy35262	XC4.2 (2016年3月22日)
Cisco TelePresence Server 8710、7010	0.CSCuy35268	4.3 (March 2016)
Cisco TelePresence Server on Multiparty Media 310、320	0.CSCuy35268	4.3 (March 2016)
Cisco TelePresence Server on Virtual Machine	0.CSCuy35268	4.3 (March 2016)
Cisco TelePresence Video Communication Server (VCS)	0.CSCuy35269	X8.7.2 (2016年3月31日)
Cisco ビデオ配信システム レコーダー	0.CSCuy35274	Affected systems have been updated.
Cisco Video Distribution Suite for Internet Streaming (VDS-IS/CDS-IS)	0.CSCuy35275	4.3.1 (2016年2月)
Cisco Video Surveillance Media Server	0.CSCuy38927	7.8 (June 2016)
Cisco Videoscape Distribution Suite Transparent Caching	0.CSCuy36594	
Cloud Object	0.CSCuy35273	Affected systems have been updated.

Store (COS)		
ワイヤレス		
Cisco Mobility Services Engine (MSE)	0.CSCuy36568	8.0.140.0 2016年4月15日)
8.1以降を実行する Cisco Wireless LAN Controller(WLC)5520	0.CSCuy36572	8.3 (2016年3月31日)
8.1以降を実行する Cisco Wireless LAN Controller(WLC)7500	0.CSCuy36572	8.3 (2016年3月31日)
8.1以降を実行する Cisco Wireless LAN Controller(WLC)8500	0.CSCuy36572	8.3 (2016年3月31日)
シスコ ホステッド サービス		
シスコ クラウド サービス	0.CSCuy38924	
Cisco Cloud Web Security	0.CSCuy36588	
Cisco Common Services Platform Collector	0.CSCuy35212	最新バージョンのglibcにアップグレードできます。
シスコ パートナー サポート サービス	0.CSCuy36463	Affected systems have been updated.
Cisco UCS Invicta Series Autosupport Portal	0.CSCuy36545	
Cisco WebEx Messenger Service	0.CSCuy36540	7.17.0 (2016年3月11日)
機能分析サービス	0.CSCuy35218	
ネットワーク変更管理 および構成管理	0.CSCuy35219	1.9 (2016年3月1日)
Smart Net Total Care (SNTC)	0.CSCuy36461	Affected systems have been updated.
Smart Net Total Care	0.CSCuy36454	Affected systems have been updated.

1. 最初の修正済みリリースより前のすべてのCisco NX-OSソフトウェアリリースは、この脆弱性の影響を受けます。

2. Cisco NX-OSソフトウェア6.0(2) Ux(x)リリースを実行しているデバイスは、この脆弱性の影響を受けません。Cisco NX-OSソフトウェア7.xリリースを実行しているデバイスは、この脆弱性の影響を受けます。

シスコの高度なマルウェア防御

Cisco Advanced Malware Protection(AMP)パブリッククラウドはCVE-2015-7547の影響を受け、パッチが適用されています。

Cisco AMPプライベートクラウドはCVE-2015-7547の影響を受け、修復機能は2016年3月31日にリリースされるバージョン2.2アップデートの一部として提供されます。

Cisco FirePower SSLアプライアンス

Cisco FirePower SSLアプライアンスデバイスは、CVE-2015-7547の影響を受けます。

Cisco StealthWatch製品

Cisco StealthWatch (旧Lancope) 製品については、[Lancope Download and License Center](#)からpatch-common-SWD6631-6.6.x-6.7.x-01.swuのパッチを入手できます。このパッチは、次の製品とバージョンに適用できます。

- StealthWatch FlowCollector – すべてのモデル、バージョン6.6.xおよび6.7.x
- StealthWatch FlowSensor – 全モデル、バージョン6.6.xおよび6.7.x
- StealthWatch Management Console : すべてのモデル、バージョン6.6.xおよび6.7.x
- StealthWatch UDP Director – すべてのモデル、バージョン6.6.xおよび6.7.x

この脆弱性およびStealthWatch Identityアプライアンスのパッチについては、次のリンク先を参照してください。 <https://www.a10networks.com/support/psirt-security-center/cve-2015-7547>

脆弱性を含まないことが確認された製品

次の製品は、このアドバイザリに記載されている脆弱性の影響を受けません。

Collaboration and Social Media

- Cisco MeetingPlace
- Cisco WebEx Node for MCS

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 Agent for OpenFlow
- Cisco AnyConnect Secure Mobility Client for Android
- Cisco AnyConnect Secure Mobility Client for Linux

- Cisco AnyConnect Secure Mobility Client for OS X
- Cisco AnyConnect Secure Mobility Client for Windows
- Cisco AnyConnect Secure Mobility Client for iOS
- Cisco IP Communicator
- Cisco Jabber Software Development Kit
- Cisco Jabber for Android
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco Jabber for iOS
- Cisco NAC Agent for Mac
- Cisco NAC Agent for Web
- Cisco UC Integration for Microsoft Lync
- Cisco WebEx Meetings for Android
- Cisco WebEx Meetings for BlackBerry
- Cisco WebEx Meetings for WP8
- Cisco WebEx Productivity Tools
- WebEx Recording Playback Client

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 ACE 30 Application Control Engine Module
- Cisco ACE 4700 シリーズ Application Control Engine Appliance
- 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 Application and Content Networking System (ACNS)
- Cisco Extensible Network Controller (XNC)
- Cisco NAC アプライアンス
- Cisco Nexus Data Broker (NDB)
- 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

- ASA CXコンテキスト認識
- Cisco ASA CX と Cisco Prime Security Manager
- Cisco Adaptive Security Device Manager
- Cisco Clean Access Manager
- Cisco Content Security Appliance Updater Servers
- Cisco Content Security Management Appliance (SMA)
- シスコ侵入防御システム (IPS)
- Cisco IronPort Email セキュリティ アプライアンス
- Cisco NAC Guest Server

- Cisco Physical Access Control Gateway
- Cisco Prime Security Manager
- Cisco Registered Envelope Service (CRES)
- Cisco Virtual Security Gateway for Microsoft Hyper-V
- Cisco Web Security Appliance (WSA)

ネットワーク管理とプロビジョニング

- Cisco Application Networking Manager
- Cisco Connected Grid Device Manager
- Cisco Connected Grid Network Management System
- Cisco Insight Reporter
- Cisco Linear Stream Manager
- Cisco MGC Node Manager (CMNM)
- Cisco Multicast Manager
- Cisco Prime Cable Provisioning
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Home
- Cisco Prime Infrastructure Standalone Plug and Play Gateway
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution (LMS - Solaris)
- Cisco Prime Network
- Cisco Prime Performance Manager
- Cisco Prime Provisioning for SPs
- Cisco Security Manager
- Cisco UCS Central
- Cisco Unified Provisioning Manager (CUPM)
- CiscoWorks Network Compliance Manager
- Local Collector Appliance (LCA)
- 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

- Cisco ASR 9000 シリーズ統合型サービス モジュール
- Cisco Broadband Access Center Telco Wireless
- ASR1K、ASR903、ISR4400、CSR1000V、CBR8K向けCisco IOS XE
- Cisco ASR 9000シリーズアグリゲーションサービスルータ向けCisco IOS XR
- Cisco CRSルータ用Cisco IOS XR
- Cisco XR 12000シリーズルータ向けCisco IOS XR

- Cisco IOS
- Cisco MDS 9000 Series Multilayer Switches
- Cisco Metro Ethernet 1200 シリーズ アクセス デバイス
- Cisco Nexus 1000V シリーズ スイッチ
- Cisco Nexus 3500 Series Switches
- Cisco Nexus 4000 Series Blade Switches
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco OnePK All-in-One VM
- Cisco Service Control Operating System
- Cisco Network Convergence System(NCS)6000向けIOS XR

ルーティングおよびスイッチング - スモール ビジネス

- Cisco DPH150シリーズMicroCellソリューション
- Cisco Small Business AP500 シリーズ ワイヤレス アクセス ポイント
- 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スイッチ
- Cisco Sx300スイッチ
- Cisco Sx500スイッチ
- Cisco WAP4410N Wireless-N Access Point

Unified Computing

- Cisco Billing and Measurementサーバ3.30
- Cisco共通暗号化モジュール
- Cisco Standalone ラック サーバ CIMC
- Cisco UCS Manager
- Cisco Unified ComputingブレードサーバCIMC
- Cisco Unified Computing System B-Series (Blade) Servers
- Cisco Unified Computing System E シリーズ ブレード サーバ

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 7937 IP Phone
- 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 Computer Telephony Integration Object Server (CTIOS)
- Cisco DX シリーズ IP フォン
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco Packaged Contact Center Enterprise
- Cisco Prime Cable Provisioning Tools Suite 5.0
- Cisco Prime Cable Provisioning Tools Suite 5.1
- Cisco Remote Silent Monitoring
- Cisco SPA112 2-Port Phone Adapter
- Cisco SPA122 ATA with Router
- Cisco SPA232D Multi-Line DECT ATA
- Cisco SPA30X Series IP Phones
- Cisco SPA50X Series IP Phones
- Cisco SPA51X Series IP Phones
- Cisco SPA525G
- 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 TAPI Service Provider (TSP)
- Cisco Unified 3900 Series IP Phones
- Cisco Unified 6901 IP フォン
- Cisco Unified 6945 IP フォン
- Cisco Unified 8831 シリーズ IP Conference Phone
- 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
- Cisco Unified Client Services Framework
- Cisco Unified Contact Center Enterprise

- Cisco Unified Contact Center Express
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 7900 Series
- Cisco Unified IP Phone 8941 および 8945 (SIP)
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified Operations Manager (CUOM)
- Cisco Unified SIP Phone 3905
- Cisco Unified Sip Proxy
- Cisco Unified Web Interaction Manager
- Cisco Unified Wireless IP Phone
- Cisco Unified Workforce Optimization
- Cisco Unity Express
- 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 (CAL)
- Cisco Command 2000 Server (cmd2k) (RH ベース)
- 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 DNCS Application Server (AppServer)
- Cisco Digital Media Players (DMP) 4300 Series
- Cisco Digital Media Players (DMP) 4400 Series
- Cisco Digital Transport Adapter Control System (DTACS)
- Cisco Download Server (DLS) (Solaris)
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco International Digital Network Control System (iDNCS)
- Cisco Media Services Interface
- Cisco Model D9485 DAVIC QPSK
- Cisco Powerkey CAS Gateway (PCG)
- Cisco Show and Share
- Cisco TelePresence 1310
- Cisco TelePresence Content Server (TCS)
- Cisco TelePresence EX Series
- Cisco TelePresence Exchange System (CTX)
- Cisco TelePresence ISDN GW 3241

- Cisco TelePresence ISDN GW MSE 8321
- Cisco TelePresence ISDN Link
- Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)
- Cisco TelePresence MX Series
- 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 Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence Serial Gateway Series
- Cisco TelePresence Supervisor MSE 8050
- Cisco TelePresence System 1000
- Cisco TelePresence System 1100
- Cisco TelePresence System 1300
- Cisco TelePresence System 3000 Series
- Cisco TelePresence System 500-32
- Cisco TelePresence System 500-37
- Cisco TelePresence TX 9000 Series
- Cisco TelePresence Integrator C Series
- Cisco Transaction Encryption Device (TED)
- Cisco VEN501 Wireless Access Point
- 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 Conductor
- Cisco Virtual PGW 2200 ソフトスイッチ
- Explorer Controller (EC) システム
- 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 3G フェムトセル ワイヤレス
- Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイント
- Cisco Mobility-Express、1800/3800アクセスポイントファミリ
- Cisco RF Gateway 1 (RFGW-1)
- Cisco Small Business 121 シリーズ ワイヤレス アクセス ポイント
- Cisco Small Business 321 シリーズ ワイヤレス アクセス ポイント
- Cisco Small Business 500 シリーズ ワイヤレス アクセス ポイント
- Cisco WAP371ワイヤレスアクセスポイント
- Cisco ワイヤレス セキュリティ ゲートウェイ アプリケーション (WSG)
- Digital Life RMS 1.8.1.1 Cisco Broadband Access Center Telco Wireless 3.8.1
- Small Cell factory recovery root filesystem V2.99.4以降

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)
- シスコのクラウドおよびシステム管理
- Cisco Connected Analytics For Collaboration
- Cisco Intelligent Automation for Cloud
- Cisco Proactive Network Operations Center
- シスコのスリム
- Cisco SMB市場
- Cisco Services Provisioning Platform (SPP)
- Cisco Smart Care
- Cisco SmartConnection
- Cisco SmartReports
- Cisco Unified Services Delivery Platform (CUSDP)
- Cisco Universal Small Cell 5000 シリーズ (V3.4.2.x ソフトウェアを実行)
- Cisco Universal Small Cell 7000 シリーズ (V3.4.2.x ソフトウェアを実行)
- Cisco Universal Small Cell usc-iuh
- Cisco WebEx Meeting Center
- Cisco WebEx ノード
- コミュニケーション/コラボレーションサイジングツール、仮想マシン配置ツール、Cisco Unified Communications Upgrade Readiness Assessment
- データセンター分析フレームワーク(DCAF)UCSコレクタ
- ICキャプチャ
- Life Cycle Management Agent Manager (LCM)
- MACD Process Controller (MPC)
- Net認証
- Network Health Framework (NHF)
- Network Performance Analytics (NPA)
- 1つのビュー

- Partner Supporting Service (PSS) 1.x
- Sentinel
- Services Analytic Platform
- サポートセントラル
- Web Element Manager

詳細

2016年2月16日に公開されたGNU glibcの脆弱性名とそれに関連するCommon Vulnerabilities and Exposures(CVE)IDは次のとおりです。

Glibc libresolvライブラリスタックベースのバッファオーバーフローの脆弱性

glibcに含まれている libresolvライブラリの脆弱性により、認証されていないリモートの攻撃者が任意のコードを実行したり、サービス妨害(DoS)状態を引き起こしたりする可能性があります。

この脆弱性は、getaddrinfo関数を使用してデュアルA/AAAA DNSクエリを実行する際のバッファの管理ミスに起因します。状況によっては、割り当てられたバッファの末尾を越えて応答が書き込まれるような方法で応答が返される場合があります。攻撃者は、巧妙に細工されたDNS応答をターゲットシステムに送信することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者が任意のコードを実行したり、DoS状態を引き起こしたりするために使用できる可能性がある、スタックベースのバッファオーバーフロー状態がトリガーされる可能性があります。

本脆弱性のIDはCVE ID CVE-2015-7547です。

回避策

回避策は今後 Cisco bugs に記載され、Cisco Bug Search Tool を使用して検索可能です。

修正済みソフトウェア

シスコがリリースした無償ソフトウェア アップデートをインストールしたり、関連するサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN .html>

また、お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキ

ユリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する場合は、<http://www.cisco.com/go/psirt> の [Cisco Security Advisories and Responses](#) アーカイブや[後続のアドバイザリ](#)を参照して、[侵害を受ける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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center (TAC) に連絡してアップグレードを入手してください。

http://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

推奨事項

```
$propertyAndFields.get("recommendations")
```

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

出典

この脆弱性は、2016年2月16日に[Red Hat](#)および[Google](#)によって公開されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160218-glibc>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.17	「脆弱性が存在する製品」セクションと「修正済みソフトウェア」セクションの用語を更新し、最新情報の参照先を明確化。	「脆弱性のある製品」、「修正済み製品」	Final	2017年 2月13日
1.16	「Cisco Unified Contact Center Express - Live Data Server」を「脆弱性が存在することが確認されている」セクションに移動。「修正済みリリース」列を更新。ドキュメントのステータスを最終に移動	該当製品	Final	2016年 6月23日
1.15	Cisco Unified Contact Center ExpressおよびCisco Converged Broadband Routers Series 8を「脆弱性を含まないことが確認された」セクションに移動。「脆弱性が存在する製品」の表のソフトウェアリリースの日付を更新。	該当製品	Interim	2016年 4月6日
1.14	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含まないことが確認された製品」のサブセクションに移動。	該当製品	Interim	2016年 3月25日
1.13	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含まないことが確認された製品」のサブセクションに移動。Cisco FirePower SSLアプライアンスの脆弱性に関する情報を追加。	該当製品	Interim	2016年 3月16日
1.12	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含まないことが確認された製品」のサブセクションに移動。	該当製品	Interim	2016年 3月9日
1.11	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含まないことが確認された製品」のサブセクションに移動。	該当製品	Interim	2016年 3月4日
1.10	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含まないことが確認された製品」のサブセクションに移動。Nexus製品の説明を追加。	該当製品	Interim	2016年 3月3日
1.9	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含まないことが確認された製品」のサブセクションに移動。	該当製品	Interim	2016年 3月2日
1.8	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含まないことが確認された製品」のサブセクシ	該当製品	Interim	2016年 3月1日

バージョン	説明	セクション	ステータス	日付
	ヨンに移動。			
1.7	調査中の製品を「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」のサブセクションに移動。「調査中」セクションを修正。「脆弱性のある製品」セクションにLancope StealthWatch製品に関する情報を追加。	該当製品	Interim	2016年 2月29日
1.6	「調査中の製品」を「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」に移動しました。Cisco Nexus 3000シリーズスイッチの該当バージョン情報を修正。	該当製品	Interim	2016年 2月26日
1.5	「調査中の製品」を「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」に移動しました。	該当製品	Interim	2016年 2月25日
1.4	「調査中の製品」を「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」に移動しました。	該当製品	Interim	2016年 2月24日
1.3	「調査中の製品」を「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」に移動しました。Cisco AMPに関する説明を追加	該当製品	Interim	2016年 2月23日
1.2	「調査中の製品」を「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」に移動しました。	該当製品	Interim	2016年 2月22日
1.1	脆弱性の範囲に関する軽微な明確化文。「調査中の製品」を「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」に移動しました。修正済みソフトウェアの提供を明確にするための文法上の軽微な変更	概要、影響を受ける製品、修正済みソフトウェア	Interim	2016年 2月19日
1.0	初回公開リリース	—	Interim	2016年 2月18日

利用規約

本アドバイザー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。本アドバイザー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、単独の転載や意識を施した場合、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。