

シスコ製品に影響を及ぼす GNU glibc の脆弱性: February 2016 年

High

アドバイザーID : cisco-sa-
20160218-glibc

[CVE-](#)
[2015-](#)
[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日で、GNU C ライブラリ (*glibc*) の業界全体、重要な脆弱性は公に表われました。

複数のシスコ製品は脆弱性から影響を受けるかもしれない *glibc* のバージョンを織込んでいます。脆弱性はリモート攻撃者非認証がサービス拒否 (DoS) 状態という結果に終るか、または攻撃者が影響を受けたデバイスの任意のコードを実行するようにするかもしれないバッファオーバーフロー状態を引き起こすように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利用できません。

このアドバイザリは、次のリンクより確認できます。

<http://tools.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。製品が影響を受けているかについて情報に関してはこのアドバイザリの「脆弱性が存在する製品」および「脆弱性が存在しない製品」セクションを参照して下さい。

「脆弱性が存在する製品」セクションは各々の影響を受けた製品のための Cisco バグ ID が含まれています。バグは [Ciscoバグ 検索ツール](#) を通してアクセス可能で、回避策 (もし可能であれば) および修正済みソフトウェアバージョンを含む追加プラットフォーム別の情報が、含まれています。

脆弱性のある製品

次のテーブルはこのアドバイザリに記載される脆弱性から影響を受けるリストし、ターゲット 発行日の間指導および修正済みソフトウェアにバージョンを提供しますシスコ製品を。

特定の修正済みソフトウェアバージョンに関する詳細な情報はこのアドバイザリの脆弱性が存在する製品 表にリストされている Ciscoバグで文書化されています。Bugs は、 [Cisco Bug Search Tool](#) で検索できます。ソフトウェアアップグレードを計画した場合、ほとんどの電流および最新情報があるのでバグを直接検討すること确实でであって下さい。

重要： その他の情報についてはについての Cisco Nexus スイッチがこの脆弱性から影響を受けるかどうか、スイッチの名前の隣で参照記号によって示されるように表の端に適切な脚注を、参照して下さい。

Product	Cisco Bug ID	Fixed Release Availability
---------	--------------	----------------------------

Collaboration and Social Media

Cisco SocialMiner	CSCuy74702	
Cisco WebEx Meetings Server versions 1.x	CSCuy36539	2.0.1.956 (31-Mar-2016) パッチは https://software.cisco.com/download/release.html? でダウンロード可能です
Cisco WebEx Meetings Server versions 2.x	CSCuy36539	2.0.1.956 (31-Mar-2016) パッチは https://software.cisco.com/download/release.html? でダウンロード可能です
Endpoint Clients and Client Software		
Cisco Jabber Guest 10.0(2)	CSCuy36613	10.6(11) (30-May-2016)
Cisco MMP サーバ	CSCuy36542	Affected systems have been updated.
Network Application, Service, and Acceleration		
Cisco Intercloud Fabric	CSCuy36549	顧客はこの脆弱性をカバーするために 2.12-166 パッチが必要です
Cisco Prime Network サービス コントローラ (PNSC)	CSCuy36549	顧客はこの脆弱性をカバーするために 2.12-166 パッチが必要です
Cisco Visual Quality Experience Server	CSCuy35276	影響を受けたシステムはアップグレードされました
Cisco Visual Quality Experience Tools Server	CSCuy35276	影響を受けたシステムはアップグレードされました
Network and Content Security Devices		
Cisco SireSIGHT IPS センサー	CSCuy32284	5.4.0.7/5.4.1.6 DC (21-March-2016) 5.4.1.6 Kenton (21-March-2016) 5.3.0./5.3.1.7 (28-March-2016)
Cisco SireSIGHT システム ソフトウェア	CSCuy32284	5.4.0.7/5.4.1.6 DC (21-March-2016) 5.4.1.6 Kenton (21-March-2016) 5.3.0./5.3.1.7 (28-March-2016)
Cisco Identity Services Engine (ISE)	CSCuy34700	2.0 P3 (4月 2016)
Cisco Physical Access Manager	CSCuy35286	影響を受けたバージョンはですアップデート (15-
Cisco Secure ACS 5.x	CSCuy36585	5.7 パッチ 2 (11-Mar-2016) 5.8 patch2 (4月 2016)
Network Management and Provisioning		
Cisco アクセスレジストラ アプリケーション	CSCuy36565	7.1 (15-Apr-2016)
Cisco Application Policy Infrastructure Controller エンタープライズ モジュール (APIC-EM)	CSCuy37090	1.1 (2016) 行進
Cisco Policy Suite (CPS)	CSCuy51595	9.1 (4月 2016)
Cisco Prime Access Registrar アプリケーション	CSCuy36565	7.1 (15-Apr-2016)
Cisco Prime Analytics	CSCuy36447	OS のための RedHat 6.5 にアップグレードして下さい
Cisco Prime Central for SPs	CSCuy36443	1.5.1 (30-March-2016)
Cisco Prime Collaboration Deployment	CSCuy36602	11.5.2 (July 2016)

Cisco Prime Data Center Network Manager (.ova および .iso インストーラ)	CSCuy36546	8.0(1) (4月 2016)
Cisco Prime IP Express	CSCuy36566	顧客は RedHat yum コーティリテイを利用する影響を受ける可能性があります。デバイスはパッケージ アップグレードする必要があります。
Cisco Prime License Manager	CSCuy35265	11.5 (6月 2016)
Cisco Prime Network Registrar (CPNR) 仮想 な アプライアンス	CSCuy36564	Affected systems have been updated.
Cisco Prime Network Registrar IP アドレス マネージャ (IPAM)	CSCuy36427	8.3 (30-Nov-2016)
Cisco Prime Optical for SPs	CSCuy36433	10.006 (31-July-2016)
Cisco Prime Service Catalog パーシャル アプライアンス	CSCuy34875	顧客は RedHat yum コーティリテイを利用する影響を受ける可能性があります。デバイスはパッケージ アップグレードする必要があります。
Cisco Unified Intelligence Center	CSCuy74698	
Cisco Videoscape Distribution Suite Service Manager	CSCuy35261	Affected systems have been updated.
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 シリーズ	CSCuy36531	18.6.0 (18-March-2016) 19.4.0 (30-June-2016) 20.0.0 (31-March-2016)
Cisco Connected Grid ルータ (CGR)	CSCuy36412	影響を受けたバージョンはですアップデート (25-15) 1(1)SG (それ以上のリリースは計画されません) 15.1(2)SG (30-Nov-2016) 15.2(1)E (それ以上のリリースは計画されません) 15.2(2)E (30-June-2016) 15.2(3)E (31-May-2016) 15.2(4)E (30-June-2016) 15.0(1)EZ (それ以上のリリースは計画されません) 15.0(1)EX (それ以上のリリースは計画されません)
Catalyst 3k のための Cisco IOS XE、4k、AIR-CT5760、Cisco RF ゲートウェイ 10 (RFGW-10)	CSCuy36597	
Cisco Nexus 1000V InterCloud	CSCuy36548	影響を受けたシステムはアップデートされます (1) 利用可能で修正します: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/1000v/1000v-uc/1000v-uc-release/notes/70322a_patch_nxos_rn.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/1000v/1000v-uc/1000v-uc-release/notes/70322b_patch_nxos_rn.html
Cisco Nexus 3016 Switch*2	CSCuy38921	利用可能で修正します: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/3000/3016/3016-release/notes/70322a_patch_nxos_rn.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/3000/3016/3016-release/notes/70322b_patch_nxos_rn.html
Cisco Nexus 3048 Switch*2	CSCuy38921	利用可能で修正します: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/3000/3048/3048-release/notes/70322a_patch_nxos_rn.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/3000/3048/3048-release/notes/70322b_patch_nxos_rn.html
Cisco Nexus 3064 シリーズ Switches*2	CSCuy38921	利用可能で修正します: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/3000/3064/3064-release/notes/70322a_patch_nxos_rn.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/3000/3064/3064-release/notes/70322b_patch_nxos_rn.html
Cisco Nexus 31128PQ スイッチ *1	CSCuy36553	パッチは利用できますで:

Cisco Emergency Responder	CSCuy36606	11.5 (6月 2016)
Cisco Finesse	CSCuy74706	
Cisco Hosted Collaboration Mediation Fulfillment	CSCuy36610	
Cisco IM and Presence Service (CUPS)	CSCuy36608	Affected systems have been updated.
Cisco MediaSense	CSCuy36619	11.5.1 (2016) 31 行進 11.0.1 (2016) 31 行進
Cisco Paging Server (Informacast)	CSCuy36612	11.5.1 (6月 2016)
Cisco Paging Server	CSCuy36612	11.5.1 (6月 2016)
Cisco Unified 7800 シリーズ IP フォン	CSCuy36620	11.5(1) (4月 2016)
Cisco Unified Communications Domain Manager	CSCuy36513	8.1.8 (July 2016)
Cisco Unified Communications Manager (UCM)	CSCuy32014	
Cisco Unified Communications Manager Session Management Edition (SME)	CSCuy32014	
Cisco Unified Contact Center Express -ライブ データ サーバ	CSCuy74701	
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	CSCuy36600	
Cisco Unity Connection (UC)	CSCuy36603	11.5 (3-Mar-2016)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco DCM Series 9900-Digital Content Manager	CSCuy35251	
Cisco Edge 300 Digital Media Player	CSCuy35298	1.6RB4_5(18-Mar-2016)
Cisco Edge 340 Digital Media Player	CSCuy35299	1.2.0.19 (31-Mar-2016)
Cisco Expressway Series	CSCuy35269	X8.7.2 (31-March-2016)
Cisco Powerkey 暗号化 サーバ (PKES)	CSCuy37232	
Cisco TelePresence Conductor	CSCuy35262	XC4.2 (22-Mar-2016)
Cisco TelePresence Server 8710、7010	CSCuy35268	4.3 (2016) 行進
Cisco TelePresence Server on Multiparty Media 310、320	CSCuy35268	4.3 (2016) 行進
Cisco TelePresence Server on Virtual Machine	CSCuy35268	4.3 (2016) 行進
Cisco TelePresence Video Communication Server (VCS)	CSCuy35269	X8.7.2 (31-March-2016)

Cisco ビデオ 伝達 システム レコーダー	CSCuy35274	Affected systems have been updated.
Cisco Video Distribution Suite for Internet Streaming (VDS-IS/CDS-IS)	CSCuy35275	4.3.1 (February 2016)
Cisco Video Surveillance Media Server	CSCuy38927	7.8 (6月 2016)
Cisco Videoscape Distribution Suite 透過型キャッシュ	CSCuy36594	
Cloud オブジェクト ストア (COS)	CSCuy35273	Affected systems have been updated.
Wireless		
Cisco モビリティ サービス エンジン (MSE)	CSCuy36568	8.0.140.0 15-Apr-2016)
Ciscoワイヤレス LAN コントローラ (WLC) 8.1 およびそれ以降を実行する 5520	CSCuy36572	8.3 (31-March-2016)
Ciscoワイヤレス LAN コントローラ (WLC) 8.1 およびそれ以降を実行する 7500	CSCuy36572	8.3 (31-March-2016)
Ciscoワイヤレス LAN コントローラ (WLC) 8.1 およびそれ以降を実行する 8500	CSCuy36572	8.3 (31-March-2016)
Cisco Hosted Services		
Cisco Cloud サービス	CSCuy38924	
Cisco Cloud Web Security	CSCuy36588	
Cisco Common Services Platform Collector	CSCuy35212	顧客は glibc の最新バージョンにアップグレードで
Cisco パートナー アフター サービス	CSCuy36463	Affected systems have been updated.
Cisco UCS Invicta Series Autosupport Portal	CSCuy36545	
Cisco WebEx Messenger Service	CSCuy36540	7.17.0 (2016) 11 行進
機能 Analytics サービス	CSCuy35218	
ネットワーク変更および設定管理	CSCuy35219	1.9 (1-March-2016)
Smart Net Total Care (SNTC)	CSCuy36461	Affected systems have been updated.
[Smart Net Total Care]	CSCuy36454	Affected systems have been updated.

- 最初の修正済みリリース以前のすべての Cisco NX-OS ソフトウェア リリースはこの脆弱性から影響を受けします。
- 実行するデバイス Cisco NX-OS ソフトウェア 6.0(2)Ux (x) リリースはこの脆弱性から影響を受けません。実行するデバイスはこの脆弱性から Cisco NX-OS ソフトウェア 7.x リリース影響を受けません。

Cisco Advanced Malware Protection

Cisco Advanced Malware Protection (AMP) 公共 Cloud は CVE-2015-7547 から影響を受け、修正されました。

Cisco AMP プライベート クラウドはバージョン 2.2 アップデートの一部として 2016 年 3 月 31 日によって利用可能であると期待される CVE-2015-7547 および治療から渡されず影響を受けません。

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 から影響を受けません。

Cisco StealthWatch 製品

Cisco StealthWatch に関しては、以前 Lancope は、製品、次のパッチ [Lancope ダウンロード](#) から現在利用でき、[ライセンスは集中します](#): patch-common-SWD6631-6.6.x-6.7.x-01.swu. このパッチは以下の製品およびバージョンに加えることができます:

- 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 -すべてのモデル、バージョン 6.6.x および 6.7.x
- StealthWatch 管理コンソール-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

この脆弱性についての情報および StealthWatch IDentity アプライアンスのためのパッチは次のリンクで利用できます: [015-7547](#)

脆弱性を含んでいないことが確認された製品

以下の製品はこのアドバイザリに記載される脆弱性から影響を受けません。

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
- OS X のための Cisco AnyConnect セキュア モビリティ クライアント
- 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)
- Content Services Switch

ネットワークおよびコンテンツ セキュリティ デバイス

- コンテキストわかっている ASA CX
- Cisco ASA CX および 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)
- Cisco 侵入防御システム ソリューション (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配置ツール

ルーティングおよびスイッチング - エンタープライズおよびサービス プロバイダー

- 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 のための Cisco IOS XE、ASR903、ISR4400、CSR1000V、CBR8K
- Cisco ASR 9000 シリーズ アグリゲーション サービス ルータのための Cisco IOS XR
- Cisco CRS ルータのための Cisco IOS XR
- Cisco XR 12000 シリーズ ルータのための Cisco IOS XR
- Cisco IOS
- Cisco MDS 9000 Series Multilayer Switches
- Cisco METRO イーサネット 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 オペレーティング システム
- Cisco ネットワーク コンバージェンス システム (NCS) のための IOS XR 6000

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 スモール ビジネス RV 120W ワイヤレス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 Sx300 switches
- Cisco Sx500 switches
- Cisco WAP4410N ワイヤレスN アクセス ポイント

Unified Computing

- Cisco Billing および Measurement サーバ 3.30
- Cisco よくある暗号 モジュール
- Cisco スタンドアロン ラック サーバ CIMC
- Cisco UCS Manager
- Cisco Unified コンピューティング 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
- ケーブル ツール スイート 4.1 のための Cisco Broadband Access Center
- ケーブル ツール スイート 4.2 のための Cisco Broadband Access Center
- 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 ツールスイート 5.0
- Cisco Prime Cable Provisioning ツールスイート 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 シリーズ IP フォン
- Cisco Unified 6901 の IP フォン
- Cisco Unified 6945 の IP フォン
- Cisco Unified 8831 シリーズ IP 会議電話
- Cisco Unified 8961 の IP フォン
- Cisco Unified 9951 の IP フォン
- Cisco Unified 9971 の 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 コマンド 2000 サーバ (cmd2k) (基づく RH)
- 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 アプリケーションサーバ (AppServer)
- Cisco Digital Media Players (DMP) 4300 Series
- Cisco Digital Media Players (DMP) 4400 Series
- Cisco デジタル トランスポート アダプタ 制御 システム (DTACS)
- Cisco ダウンロード サーバ (DLS) (Solaris)
- Cisco Enterprise Content Delivery System (ECDS)
- Digital Network Control System (DNCS) Cisco インターナショナル (iDNCS)
- Cisco Media Services Interface
- Cisco Model D9485 DAVIC QPSK
- Cisco Powerkey CAS ゲートウェイ (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
- Transaction Encryption Device (TED) IV Cisco (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
- エクスプローラ コントローラ (EC) システム
- Tandberg Codian ISDN GW 3210/3220/3240
- Tandberg Codian MSE 8320 model
- VDS レコーダー
- GW をキャッシュする VDS-TV
- VDS-TV 吹流し
- VDS-TV 地下

ワイヤレス

- Cisco 3G Femtocell 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 のアクセス ポイント ファミリー
- Cisco RF ゲートウェイ 1 (RFGW-1)
- Cisco スモール ビジネス 121 シリーズ ワイヤレスアクセスポイント
- Cisco スモール ビジネス 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)
- デジタル ライフ RMS 1.8.1.1 Cisco Broadband Access Center Telco ワイヤレス 3.8.1
- 小さいセル ファクトリ リカバリ ルート ファイルシステム V2.99.4 およびそれ以降

シスコ ホステッド サービス

- ビジネス ビデオは保守しますオートメーション ソフトウェア (BV) を
- Cisco クラウドおよびシステム管理
- Cisco Connected Analytics for Collaboration
- Cisco Intelligent Automation for Cloud
- Cisco 予防的 な Network Operations Center
- 細い Cisco
- Cisco SMB 市場
- Cisco Services Provisioning Platform (SPP)
- Cisco スマートな注意
- 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 ユニバーサル小さいセル usc-iuh
- Cisco WebEx Meeting Center
- Cisco WebEx ノード
- 通信/コラボレーション サイズ変更ツールは、仮想マシン配置 ツール、Cisco Unified Communications 準備の評価をアップグレードします
- データセンター アナリティクス フレームワーク (DCAF) UCS 収集装置
- ICS キャプチャ
- ライフサイクル 管理 エージェント マネージャ (LCM)
- MACD プロセス コントローラ (MPC)
- NetAuthenticate
- Network Health Framework (NHF)
- Network Performance Analytics (NPA)
- 1 つのビュー
- Partner Supporting Service (PSS) 1.x
- センチネル
- サービス分析プラットフォーム
- サポート本部
- Web Element Manager

詳細

脆弱性名前および関連するよくある脆弱性および公開 (のための CVE) ID は 2016 年 2 月 16 日、GNU *glibc* 公開次の通りです。

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

glibc と含まれていた *libresolv* ライブラリの脆弱性は非認証、リモート攻撃者が任意のコードを実行するか、またはサービス拒否 (DoS) 状態を引き起こすことを可能にする可能性があります。

脆弱性は二重 A/AAAA DNS クエリを行うのに *getaddrinfo* 機能が使用されているとき不始末をバッファリングして当然です。ある状況では、応答はある意味では返されるかもしれませんが応答を割り当てられたバッファの端を過ぎて書きます。攻撃者はターゲットのシステムへの巧妙に細工された DNS 応答の送信によってこの脆弱性を不正利用する可能性があります。不正利用の成功は任意のコードを実行するか、または DoS 状態を引き起こすのに使用する攻撃者が可能性があるスタックベース バッファオーバーフロー状態を引き起こす可能性があります。

この脆弱性には次の CVE ID が割り当てられています。CVE-2015-7547

セキュリティ侵害の痕跡

回避策

どの回避策でも [Ciscoバグ 検索ツール](#)を通してアクセス可能である Ciscoバグで文書化されています。

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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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>

さらに、顧客は彼らに有効なライセンスがある Cisco からまたは Cisco 認定 再販業者かパートナーを通して直接手に入れられるソフトウェア ダウンロードだけかもしれないです。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。無償のセキュリティ 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/en/US/support/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。

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エクスプロイト事例は確認していません。

出典

この脆弱性は [Red Hat および Google によって公に](#) 2016 年 2 月 16 日 [表われました](#)。

URL

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160218-glibc>

改訂履歴

Version	Description	Section	Status	日付
1.17	明白にする脆弱性が存在する製品および修正済みソフトウェアのセクションの更新済言語最新情報のために行くためにどこに。	脆弱性が存在する製品、固定製品	Final	2017-February-13
1.16	移動された Cisco Unified Contact Center Express - 確認された脆弱なセクションへのライブデータサーバ。更新済修正済みリソースカラム。最終への移動された文書ステータス	該当製品	Final	2016-June-23
1.15	移動された Cisco Unified Contact Center Express および Cisco はシリーズ 8 確認された脆弱ではないセクションにブロードバンドルータコンバージしました。脆弱性が存在する製品表の更新済ソフトウェアのリリース日。	影響を受けた Products	Interim	2016-April-06
1.14	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-March-25
1.13	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。Cisco Firepower SSL アプライアンスのための追加された脆弱性情報。	該当製品	Interim	2016-March-16
1.12	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-March-09

1.11	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-March-04
1.10	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。Nexus 製品のための追加された説明。	該当製品	Interim	2016-March-03
1.9	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-March-02
1.8	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-March-01
1.7	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。調査中のセクションを訂正しました。脆弱性が存在する製品 セクションへの Lancope StealthWatch 製品についての追加された情報。	該当製品	Interim	2016-February-29
1.6	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。Cisco Nexus 3000 シリーズ スイッチの訂正された影響を受けたバージョン情報。	該当製品	Interim	2016-February-26
1.5	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-February-25
1.4	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-February-24
1.3	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。Cisco AMP についての追加された文。	該当製品	Interim	2016-February-23
1.2	脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。	該当製品	Interim	2016-February-22
1.1	脆弱性のスコープのためのマイナー な明白になる文。脆弱性が存在する製品または脆弱性が存在しない製品サブセクションに調査中の移動された製品。修正済みソフトウェアが迫っていること明白になるべきマイナー な文法変更。	要約、該当製品、修正済みソフトウェア	Interim	2016-February-19
1.0	Initial public release.		Interim	2016-February-18

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。

本アドバイザー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。