Multiple Vulnerabilities in ntpd Affecting Cisco Products

Advisory ID：cisco-sa-20141222-ntpd

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141222-ntpd

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。

Revision 2.10

Last Updated 2015 March 31 15:29 UTC (GMT)

For Public Release 2014 December 22 16:00 UTC (GMT)

目次

要約

複数のシスコ製品に *ntpd* パッケージが統合されています。このパッケージには脆弱性が 1 つまたは複数存在するため、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、DoS 状態を発生させたりする可能性があります。

2014 年 12 月 19 日に NTP.org と US-CERT が発表したセキュリティ アドバイザリで、暗号化における弱い疑似乱数生成器（PRNG）に関する 2 つの問題、バッファ オーバーフローに関する 3 つの脆弱性、および影響が不明な未処理のエラー条件について詳しく解説されました。この脆弱性は、本ドキュメントで次のように言及されています。

- CVE-2014-9293：config_auth() における弱いデフォルト キー
- CVE-2014-9294：ntp-keygen が弱いシードを持つ非暗号乱数生成器を使用して対称キーを生成
- CVE-2014-9295：ntpd に存在する複数のバッファ オーバーフローの脆弱性

- CVE-2014-9296：ntpd receive()：エラー時の Return の欠落

2015 年 2 月 4 日、NTP.org と US-CERT は *ntp_crypto.c* 内の不適切な *vallen* と IPv6 ::1 ACL バイパスについての 2 つの追加の脆弱性についてのリリースを行い、オリジナルのアドバイザリに追加されました。 これらの脆弱性は以下のように言及されています。

- CVE-2014-9297: NTP ntp_crypto.c での不適切な検証の脆弱性
- CVE-2014-9298: NTP IPv6 ACL バイパスの脆弱性

追加情報があり次第、このアドバイザリは更新されます。

シスコは、これらの脆弱性に対応するための無償ソフトウェア アップデートをリリースする予定です。

これらの脆弱性に対しては回避策があります。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141222-ntpd

該当製品

脆弱性が認められる製品

CVE-2014-9295

Product	Defect	Fixed releases availability
Collaboration and Social Media		
Cisco Unified MeetingPlace	CSCus27576	Patch available for 8.6 (27-Feb-15) Patch available for 8.5 MR3 (27-Feb-15)
Cisco WebEx Social	CSCus27488	No further releases planned.
Network Application, Service, and Acceleration		
Cisco Application and Content Networking System (ACNS)	CSCus26947	ACNS 5.5.39
Cisco Wide Area Application Services (WAAS)	CSCus26864	5.5.3 (25-Mar-2015) 5.5.3d (31-May-2015)
Network and Content Security Devices		
Cisco ASA CX and Cisco Prime Security Manager	CSCus27226	9.3.3.2 (1-May-15)
Cisco FireSIGHT System Software	CSCus27325	4.10.3.11 5.2.0.8 5.4.0.1 5.3.1.2 5.3.0.3
Cisco IronPort Encryption Appliance (IEA)	CSCus27240	No further releases planned.
Cisco Physical Access Gateway	CSCus27369	1.5(3.0.3.2) (15-April-2015)
Cisco Virtual Security Gateway	CSCus27283	5.2(1)VSG2(1.1)
Network Management and Provisioning		
Cisco Application Networking Manager	CSCus27501	Update via Admin Shell
Cisco Common Services Platform Collector	CSCus27536	1.4
Cisco Digital Media Manager (DMM)	CSCus26895	5.6
Cisco Intelligent Automation for Cloud	CSCus27302	4.2

Cisco NetFlow Collection Agent	CSCus27340	001.003(000.000)
Cisco Physical Access Manager	CSCus27373	1.5.3 (3-Apr-2015)
Cisco Prime Data Center Network Manager (.ova and .iso installers)	CSCus27527	Update via Admin Shell
Cisco Prime Infrastructure	CSCus27337	Patch update available for vulnerable releases.
Cisco Prime LAN Management Solution (Linux Bundles)	CSCus27300	MR3 - 004.002(005.003) (End of April , 2015)
Cisco Prime License Manager	CSCus27292	11.0 (May 2015)
Cisco Prime Service Catalog Virtual Appliance	CSCus27577	Update via Admin Shell
Cisco Quantum Policy Suite (QPS)	CSCus27432	7.5 (Available 30-Jun-2015)
Cisco Quantum SON Suite	CSCus27433	Update via Admin Shell
Cisco Unified Provisioning Manager 8.6 on Linux	CSCus43427	No further releases planned.
Prime Collaboration Provisioning	CSCus27270	11.0 (22-Jun-2015)
Routing and Switching - Enterprise and Service Provider		
Cisco Application Policy Infrastructure Controller	CSCus27224	1.0(3)
Cisco IOS XR Software (NCS6K, NCS4K,ASR9K, CRS, C12K)	CSCus26956	5.3.1
Cisco MDS 9000 Series Multilayer Switches	CSCus27221	5.2(8f) 6.2(11b)
Cisco Nexus 1000V Series Switches	CSCus26882	5.2(1)SV3(1.2.105)
Cisco Nexus 3000 Series Switches	CSCus26875	6.0(2)U6(1) 6.0(2)U5(2) 6.0(2)U4(4) 6.0(2)A6(1) 6.0(2)A5(2) 6.0(2)A4(4)
Cisco Nexus 4000 Series Switches	CSCus26859	4.1(2)E1(1o)
Cisco Nexus 5000 Series Switches	CSCus26870	7.0(6)N1(1) 5.2(1)N1(8b)
Cisco Nexus 6000 Series Switches	CSCus26873	7.0(6)N1(1)
Cisco Nexus 7000 Series Switches	CSCus26870	6.2(12)
Cisco Nexus 9000 Series Switches	CSCus29415	7.0(3)I1(1)
Cisco OnePK All-in-One VM	CSCus27274	Update via Admin Shell
Cisco Service Control Operating System	CSCus27279	Patch file available for Cisco Service Control Engine 1000 Series versions 5. to 5.1.0 (5-Apr-2015) Patch file available for Cisco Service Control Engine 8000 Series versions 3. to 5.1.0 (5-Apr-2015) 5.2.0 (Available 31-Aug-2015)
IOS-XR for Cisco Network Convergence System (NCS) 6000	CSCus27229	AA09409: NCS6K-sysadmin5.0.1 AA09410: NCS6K-sysadmin5.2.1
Unified Computing		
Cisco UCS Director	CSCus27245	Patch files are available for vulnerable releases.
Cisco UCS Invicta Series	CSCus27263	5.0(1.3a) (Release date pending CentOS fix) 5.0(1.2b) (Release date pending CentOS fix)
Voice and Unified Communications Devices		
Cisco Emergency Responder	CSCus27391	11.0
Cisco Finesse	CSCus27243	11.0 (June 2015)
Cisco IM and Presence Service (CUPS)	CSCus27395	9.1.1 SU5 (10th April 2015) 10.5.1 SU3 (27th March 2015) 10.5.2 SU1 (20th March 2015)
Cisco IP Interoperability and Collaboration System (IPICS)	CSCus26891	ipics-os-security_patch-8.0-0_el5.bin (15-Feb-15)

Cisco Jabber Guest	CSCus27589	10.6 (24-Apr-15)
Cisco Management Heartbeat Server	CSCus27595	SR10 (13-Feb-15) RMS 4.1 (13-Feb-15) RMS 5.0 (13-Feb-15)
Cisco MediaSense	CSCus27244	11.0(1) (July 2015) 10.5(1)SU1
Cisco Paging Server (Informacast)	CSCus27269	9.0.1
Cisco Paging Server	CSCus27269	9.0.1
Cisco Unified Communications Domain Manager	CSCus27222	10.1(2)
Cisco Unified Communications Manager (CUCM)	CSCus26858	10.5(2)su1 (Available) 9.1(2)su3 (April 2015)
Cisco Unified Contact Center Express (UCCX)	CSCus26946	11.0(1) (Available 30-Jun-15)
Cisco Unified Intelligence Center (CUIC)	CSCus27247	11.0(1) (June 2015)
Cisco Unity Connection (UC)	CSCus27364	8.6(2)ES163 (Available) 9.1(2)ES82 (Available) 10.5(2)ES11 (Available)
Cisco Universal Small Cell RAN Management System Wireless	CSCus27596	RMS4.1.0
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco AutoBackup Server	CSCus27553	OS is not distributed with product. Check with OS vendor for fixes.
Cisco Command 2000 Server (cmd2k)	CSCus27551	Update with latest version supplied by Oracle.
Cisco Common Download Server (CDLS)	CSCus27561	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco D9036 Modular Encoding Platform	CSCus27255	V02.03.214
Cisco DCM Series 9900-Digital Content Manager	CSCus27291	V16.0 (1-Apr-15)
Cisco DNCS Application Server (AppServer)	CSCus27562	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Digital Network Control System (DNCS)	CSCus27535	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Digital Transport Adapter Control System (DTACS)	CSCus27560	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Download Server (DLS) (Linux Based)	CSCus27554	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Download Server (DLS) (Solaris Based)	CSCus27558	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Edge 300 Digital Media Player	CSCus27239	1.7 (16-Mar-2015)
Cisco Enterprise Content Delivery Service	CSCus27241	2.6.4 (30-Apr-2015)
Cisco Explorer Controller (EC) server	CSCus37392	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco IPTV Service Delivery System (ISDS)	CSCus27555	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco International Digital Network Control System (iDNCS)	CSCus27556	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Media Experience Engines (MXE)	CSCus30138	3.5 (April 2015)
Cisco PowerVu D9190 Conditional Access Manager (PCAM)	CSCus27458	v1.1.0 (31-Mar-2015)
Cisco PowerVu Network Center	CSCus27620	Update via Admin Shell
Cisco PowerKey Encryption Server (PKES)	CSCus27550	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Remote Conditional Access System (RCAS)	CSCus27557	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Remote Network Control System (RNCS)	CSCus27548	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Show and Share	CSCus27253	5.6 (March 2015)
Cisco TelePresence 1310	CSCus27281	6.1.7 (March 2015)

Cisco TelePresence Endpoints (C series, EX series, MX series, MXG2 series, SX series) and the 10" touch panel	CSCus27007	7.3.1
Cisco TelePresence System 1000	CSCus27281	6.1.7 (March 2015)
Cisco TelePresence System 1100	CSCus27281	6.1.7 (March 2015)
Cisco TelePresence System 1300	CSCus27281	6.1.7 (March 2015)
Cisco TelePresence System 3000 Series	CSCus27281	6.1.7 (March 2015)
Cisco TelePresence System 500-32	CSCus27281	6.1.7 (March 2015)
Cisco TelePresence System 500-37	CSCus27281	6.1.7 (March 2015)
Cisco TelePresence TE Software (for E20 - EoL)	CSCus27309	No further planed software releases scheduled.
Cisco TelePresence TX 9000 Series	CSCus27281	6.1.7 (March 2015)
Cisco Transaction Encryption Device (TED)	CSCus27547	Patch files available for vulnerable releases. (3-Mar-2015)
Cisco Video Delivery System Recorder	CSCus62967	3.4.2 (15-Feb-2015) 3.8.1 (15-Feb-2015) or Update via Admin Shell
Cisco Video Surveillance Media Server	CSCus27388	7.7 (Oct 2015)
Cisco Videoscape Conductor	CSCus27345	Update with latest version supplied by Red Hat.
Cisco Virtualization Experience Client 6215	CSCus27483	End of Life. No future releases are forthcoming.
Cloud Object Store (COS)	CSCus27358	2.1.1 (15-Feb-2015) 2.1.2 (15-Feb-2015) 2.1.3 (15-Feb-2015) or Update via Admin Shell
Cisco Hosted Services		
Cisco Network Configuration and Change Management Service	CSCus27470	Update via Admin Shell

CVE-2014-9297 CVE-2014-9298

Product	Defect	Fixed releases availability
Network and Content Security Devices		
Cisco Physical Access Gate	CSCus27369	1.5(3.0.3.2) (15-April-2015)

way		
Network Management and Provisioning		
Cisco Prime Data Center Network Manager (.ova and .iso installers)	CSCus88284	7.1(2)PF (31-Mar-2015)
Cisco QuA	CSCus27432	7.5 (Available 30-Jun-2015)

rtuPolicySuite(QPS)		
Cisco Virtual Systems Operations Center Enforcement Project	CSCus94209	2.0 (1-Apr-2015) Note: Not affected by other NTP vulnerabilities.
Unified Computing		

Cisco UCS Director	CSCus90552	Software and release date pending CentOS fix.
Cisco UCS Invicta Series	CSCus27263	5.0(1.3a) (Release date pending CentOS fix) 5.0(1.2b) (Release date pending CentOS fix)
Voice and Unified Communications Devices		
Cisco Jabber Guest	CSCus88292	Update via Admin Shell 10.6.5
Cisco Management	CSCus89695	SR10 (13-Feb-15) RMS 4.1 (13-Feb-15) RMS 5.0 (13-Feb-15)

Heartbeat Server		
Cisco Universal Small Cell RAN Management System Wireless	CSCus27596	SR10 (3-Mar-2015) RMS4.1 (3-Mar-2015) RMS5.0 (3-Mar-2015)
Video, Streaming, TelePresence, and Transcoding Devices		
Cis	CSCus88487	7.3.2

coTelePresence Endpoints (C series, EX series, MX series, MXG2 series, SX series)		

another "touch panel		
Cisco TelePresence TE Software (for C-Series)	CSCus90674	TE 4.1.6 (April 2015)
Cisco VideoDe	CSCus62967	Update via Admin Shell

Inventory System Reconcile		
Cisco Video Surveillance Backoffice (VSBO)	CSCus82885	V4.0-Branch (27-Mar-2015)
Cloud Object Storage (COS)	CSCus27358	2.1.1 (15-Feb-2015) 2.1.2 (15-Feb-2015) 2.1.3 (15-Feb-2015) or Update via Admin Shell

脆弱性が認められない製品

CVE-2014-9297 および CVE-2014-9298 の影響を受けないもの

分析の結果、次のシスコ製品とサービスは CVE-2014-9295 の影響を受けるが CVE-2014-9297 および CVE-2014-9298 の影響を受けないことが判明しています。

Collaboration and Social Media

- Cisco Unified MeetingPlace
- Cisco WebEx Social

Network and Content Security Devices

- Cisco ASA CX and Cisco Prime Security Manager
- Cisco FireSIGHT System Software
- Cisco IronPort Encryption Appliance (IEA)
- Cisco Virtual Security Gateway

Network Application, Service, and Acceleration

- Cisco Application and Content Networking System (ACNS)
- Cisco Wide Area Application Services (WAAS)

Network Management and Provisioning

- Cisco Common Services Platform Collector
- Cisco Digital Media Manager (DMM)
- Cisco Intelligent Automation for Cloud
- Cisco Prime LAN Management Solution (Linux Bundles)
- Cisco Prime License Manager
- Cisco Prime Service Catalog Virtual Appliance
- Cisco Quantum SON Suite
- Cisco Unified Provisioning Manager 8.6 on Linux

Routing and Switching - Enterprise and Service Provider

- Cisco Application Policy Infrastructure Controller
- Cisco IOS XR Software (NCS6K, NCS4K,ASR9K, CRS, C12K)
- Cisco MDS 9000 Series Multilayer Switches
- Cisco Nexus 1000V Series Switches
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 4000 Series Switches
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 Series Switches
- Cisco OnePK All-in-One VM

- Cisco Service Control Operating System
- IOS-XR for Cisco Network Convergence System (NCS) 6000

Network Management and Provisioning

- Cisco Application Networking Manager
- Cisco Netflow Collection Agent
- Cisco Physical Access Manager
- Prime Collaboration Provisioning
- Cisco Prime Infrastructure

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco AutoBackup Server
- Cisco Command 2000 Server (cmd2k)
- Cisco Common Download Server (CDLS)
- Cisco D9036 Modular Encoding Platform
- Cisco DCM Series 9900-Digital Content Manager
- Cisco Digital Network Control System (DNCS)
- Cisco Digital Transport Adapter Control System (DTACS)
- Cisco DNCS Application Server (AppServer)
- Cisco Download Server (DLS) (Linux Based)
- Cisco Edge 300 Digital Media Player
- Cisco Emergency Responder
- Cisco Enterprise Content Delivery Service
- Cisco Explorer Controller (EC) server
- Cisco IPTV Service Delivery System (ISDS)
- Cisco International Digital Network Control System (iDNCS)
- Cisco Media Experience Engines (MXE)
- Cisco PowerKey Encryption Server (PKES)
- Cisco PowerVu D9190 Conditional Access Manager (PCAM)
- Cisco PowerVu Network Center
- Cisco Remote Conditional Access System (RCAS)
- Cisco Remote Network Control System (RNCS)
- Cisco Show and Share
- Cisco TelePresence System 1000
- Cisco TelePresence System 1100
- Cisco TelePresence System 1300
- Cisco TelePresence 1310
- Cisco TelePresence System 3000 Series
- Cisco TelePresence System 500-32
- Cisco TelePresence System 500-37
- Cisco TelePresence TX 9000 Series
- Cisco Transaction Encryption Device (TED)
- Cisco Videoscape Conductor
- Cisco Video Surveillance Media Server
- Cisco Virtualization Experience Client 6215

Voice and Unified Communications Devices

- Cisco Finesse
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco IM and Presence Service (CUPS)
- Cisco MediaSense
- Cisco Paging Server (Informacast) (ntp support was removed with Cisco bug ID CSCus27269)
- Cisco Paging Server (ntp support was removed with Cisco bug ID CSCus27269)
- Cisco Unified Communications Domain Manager
- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Contact Center Express (UCCX)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unity Connection (UC)

Cisco Hosted Services

- Cisco Network Configuration and Change Management Service

いずれの脆弱性の影響も受けないもの

分析の結果、次のシスコ製品およびサービスはいずれの脆弱性の影響も受けないことが分かっています。

Collaboration and Social Media

- Cisco WebEx Meeting Server versions 2.x

Endpoint Clients and Client Software

- Cisco IP Communicator
- Cisco Jabber for Android
- Cisco Jabber for iOS
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- 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 Application Control Engine (ACE10 and ACE20)
- Cisco Application Control Engine (ACE30/ACE 4710)
- Cisco Clean Access Manager
- Cisco Extensible Network Controller (XNC)
- Cisco GSS 4492R Global Site Selector
- Cisco NAC Guest Server
- Cisco NAC Server
- Content Services Switch

- Cisco Smart Call Home
- Cisco Visual Quality Experience Server
- Cisco Visual Quality Experience Tools Server
- Openflow Agent

Network and Content Security Devices

- Catalyst 6500 Series / 7600 Series ASA Services Module
- Cisco Adaptive Security Appliance (ASA)
- Cisco Adaptive Security Device Manager
- Cisco Content Security Appliance Updater Servers
- Cisco Email Security Appliance (ESA)
- Cisco Firewall Services Module (FWSM)
- Cisco Identity Services Engine (ISE)
- Cisco Intrusion Prevention System Solutions (IPS)
- Cisco Secure Access Control Server (ACS)
- Cisco Security Management Appliance (SMA)
- Cisco Web Security Appliance (WSA)

Network Management and Provisioning

- Cisco Cloud Consumption Service collector
- Cisco Connected Grid Network Management System
- Network Device Security Assessment
- Cisco Insight Reporter
- Cisco Local Collector Appliance (LCA)
- Cisco MATE collector
- Cisco MATE Design
- Cisco MATE Live
- Cisco Mobile Wireless Transport Manager
- Cisco Multicast Manager
- Cisco Network Analysis Module
- Cisco Network Collector
- CiscoWorks Network Compliance Manager
- Cisco Prime Access Registrar
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Collaboration Assurance
- Cisco Prime Data Center Network Manager (Windows and Linux)
- Cisco Prime Home
- Cisco Prime IP Express
- Cisco Prime Network
- Cisco Prime Network Registrar (CPNR)
- Cisco Prime Network Services Controller
- Cisco Prime Optical for SPs
- Cisco Prime Performance Manager
- Cisco Prime Provisioning

- Cisco Security Manager
- Cisco UCS Central
- Cisco Unified Communications Deployment Tools
- Cisco Unified Provisioning Manager (CUPM)
- DCAF UCS Collector
- Network Profiler
- Security Module for Cisco Network Registrar
- Virtual Systems Operations Centre for vPE Project

Routing and Switching - Enterprise and Service Provider

- Cisco ASR 5000 Series
- Cisco ASR 9000 Series Integrated Service Module
- Cisco Connected Grid Device Manager
- Cisco Connected Grid Routers (CGR)
- Cisco IOS Software
- Cisco IOS XE for ASR1k, ASR903, ISR4400, and CSR1000v
- Cisco IOS XE for Catalyst 3k, 4k, AIR-CT5760, and Cisco RF Gateway 10 (RFGW-10)
- Cisco Metro Ethernet 1200 Series Access Devices
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco Quantum Virtualized Packet Core
- Cisco Service Control Application for Broadband
- Cisco Service Control Collection Manager
- Cisco Service Control Subscriber Manager
- Cisco VPN Acceleration Engine
- CRS-CGSE-PLIM
- CRS-CGSE-PLUS

Routing and Switching - Small Business

- Cisco DPH150 Series MicroCell Solution
- Cisco Sx220 Switches
- Cisco Sx300 Switches
- Cisco Sx500 Switches
- 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 Series Routers 0xxv3
- Cisco Small Business RV Series Routers RV110W
- Cisco Small Business RV120W Wireless-N VPN Firewall
- Cisco Small Business RV Series Routers RV130x
- Cisco Small Business RV Series Routers RV215W
- Cisco Small Business RV Series Routers RV220
- Cisco Small Business RV Series Routers RV220W
- Cisco Small Business RV Series Routers RV315W
- Cisco Small Business RV Series Routers RV320
- Cisco WAG310G Residential Gateway

Unified Computing

- Cisco Standalone Rack Server CIMC
- Cisco UCS ADA
- Cisco UCS Manager
- Cisco Unified Computing System B-Series Blade Servers
- Cisco Unified Computing System E-Series Blade Servers

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco AnyRes VOD (CAV)
- Cisco AnyRes Live (CAL)
- Cisco Broadband Access Center for Cable Tools Suite
- Cisco Broadband Access Center Telco Wireless
- 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 Edge 340 Digital Media Player
- Cisco IPTV
- 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 TelePresence Advanced Media Gateway Series
- Cisco TelePresence Conductor
- Cisco TelePresence Content Server (TCS)
- Cisco TelePresence Exchange System (CTX)
- Cisco TelePresence IP Gateway Series
- Cisco TelePresence IP VCR Series
- Cisco TelePresence ISDN GW 3241
- Cisco TelePresence ISDN GW MSE 8321
- Cisco TelePresence ISDN Link
- Cisco TelePresence Manager (CTSMan)
- 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 MCU (8510, 8420, 4200, 4500 and 5300)
- Cisco TelePresence MPS Series
- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence MXP Software

- Cisco TelePresence Recording Server (CTRS)
- 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 TelePresence Video Communications Server (VCS)
- Cisco VDS Service Broker
- Cisco Videoscape Back Office (VBO): Note: Has a ntp.conf configuration that makes it vulnerable to CVE-2014-9297.
- Cisco Video Distribution Suite
- Cisco Videoscape Distribution Suite Transparent Caching
- 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 Virtual PGW 2200 Softswitch
- Digital Media Player (DMP) 4310
- Digital Media Player (DMP) 4400
- Media Services Interface
- Tandberg Codian ISDN GW 3210/3220/3240
- Tandberg Codian MSE 8320 model

Voice and Unified Communications Devices

- Cisco 190 ATA Series Analog Terminal Adapter
- Cisco 7937 IP Phone
- Cisco ATA 187 Analog Telephone Adapter
- Cisco Agent Desktop
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco Desktop Collaboration Experience DX650
- Cisco Desktop Collaboration Experience DX70 and DX80
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco IP Phone 8800 Series
- Cisco MS200X Ethernet Access Switch
- Cisco Unified Workforce Optimization
- Cisco Unity Express
- 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 SPA8800 IP Telephony Gateway with 4 FXS and 4 FXO Ports
- Cisco SPA30X Series IP Phones
- Cisco SPA50X Series IP Phones
- Cisco SPA51X Series IP Phones

- Cisco SPA525G Series IP Phones
- Cisco SPA8000 8-port IP Telephony Gateway
- Cisco Social Miner
- Cisco TAPI Service Provider (TSP)
- Cisco Unified 3900 Series IP Phones
- Cisco Unified 6900 Series IP Phones
- Cisco Unified 6911 IP Phone
- Cisco Unified 6945 IP Phone
- Cisco Unified 7800 Series IP Phones
- Cisco Unified 7900 Series IP Phones
- Cisco Unified 8941 IP Phone
- Cisco Unified 8945 IP Phone
- 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
- Cisco Unified Contact Center Enterprise
- Cisco Unified Client Services Framework
- Cisco Unified Communications Widgets Click To Call
- Cisco Unified Email Interaction Manager
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified Integration for IBM Sametime
- Cisco Unified IP Conference Phone 8831
- Cisco Unified Operations Manager (CUOM)
- Cisco Unified Service Monitor
- Cisco Unified Service Statistics Manager
- Cisco Unified SIP Proxy
- Cisco Unified Customer Voice Portal
- Cisco Unified Web Interaction Manager
- Cisco Unified Wireless IP Phones
- Cisco Virtualization Experience Media Engine
- Xony VIM/CCDM/CCMP

Wireless

- Cisco Mobility Services Engine (MSE)
- Cisco RF Gateway 1 (RFGW-1)
- Cisco Mobility Services Engine
- Cisco Small Business 121 Series Wireless Access Points
- Cisco Small Business 321 Series Wireless Access Points
- Cisco Small Business 371 Series Wireless Access Points
- Cisco Small Business 500 Series Wireless Access Points
- Cisco Wireless Control System (WCS)

- Cisco Wireless LAN Controller (WLC)
- Cisco Wireless Security Gateway Application (WSG)

Cisco Hosted Services

- Business Video Services Automation Software (BV)
- Cisco Discovery Service
- Cisco Connected Analytics For Collaboration
- Cisco Cloud and Systems Management
- Cisco Cloud Email Security
- Cisco Cloud Services
- Cisco Cloud Web Security (CWS)
- Cisco Install Base Management
- Cisco Partner Supporting Service
- Cisco Proactive Network Operations Center
- Cisco Registered Envelope Service (CRES)
- Cisco Services Platform Collector (CSPC)
- Cisco Services Provisioning Platform (SPP)
- Cisco Smart Care
- Cisco Smart Connection
- Cisco Smart Reports
- Cisco Smart Net Total Care (SNTC)
- Cisco SMB Market Place
- Cisco UCS Invicta Series Autosupport Portal
- Cisco Unified Communications Sizing Tool
- Cisco Unified Services Delivery Platform (CUSDP)
- Cisco Universal Small Cell 5000 Series running V3.4.2.x software
- Cisco Universal Small Cell 7000 Series running V3.4.2.x software
- Cisco Universal Small Cell CloudBase
- Cisco WebEx Connect client (Windows)
- Cisco WebEx Messenger Service
- Cisco WebEx Meetings for Android
- Cisco WebEx Meetings for BlackBerry
- Cisco WebEx Meetings for iOS
- Cisco WebEx Meetings for WP8
- Cisco WebEx Node for MCS
- Cisco WebEx Productivity Tools
- Cisco WebEx WebOffice & Workspace
- Connected Analytics for Network Deployment (CAND)
- Data Center Analytics Framework (DCAF)
- Feature Analytics Service
- Femto Provisioning Gateway
- MACD Process Controller (MPC)
- Network Health Framework (NHF)
- Network Performance Analytics (NPA)
- One View
- On Going Support Automation (OGSA)
- Serial Number Assessment Service (SNAS)

- SI component of Partner Supporting Service
- Small Cell Factory Recovery Root Filesystem V2.99.4 or later
- Support Central
- Unified Communication Audit Tool (UCAT)
- WebEx Meeting Center
- WebEx PCNow
- WebEx QuickBooks
- WebEx Recording Playback

このセクションは、各製品の調査が終了に伴い随時更新されます。

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

2014 年 12 月 19 日に NTP.org と US-CERT が発表した *ntpd* についてのセキュリティ アドバイザリで、暗号化における弱い疑似乱数生成器（PRNG）に関する 2 つの問題、バッファ オーバーフローに関する 3 つの脆弱性、および影響が不明な未処理のエラー条件について詳しく解説されています。さらに、2015 年 2 月 4 日、このアドバイザリに自動鍵更新と IPv6 ACL バイパスについての脆弱性が追加されました。

これら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可能性があります。

シスコ製品については、本ドキュメントの「該当製品」リストの Cisco Bug ID 情報を参照してください。

追加情報や詳しい手順は、シスコの各製品のインストール ガイド、コンフィギュレーション ガイド、メンテナンス ガイドに記載されています。さらに説明やアドバイスが必要な場合、サポート担当者にお問い合わせください。

脆弱性の名称およびそれらに関連する Common Vulnerabilities and Exposures（CVE）ID は、次のとおりです。

- config_auth() における弱いデフォルト キー
- *ntpd* 用のランダム キーの生成に問題があるため、認証されていないリモートの攻撃者が生成されたキーの推測に成功する可能性があります。攻撃者はこれを使って *ntpdc* クエリまたはコンフィギュレーション リクエストを送信する可能性があります。

  この問題の原因は、*ntp.conf* コンフィギュレーション ファイルで *ntpdc* 要求認証キーが指定されていない場合、*ntpd* が自動的に弱いキーを生成することです。攻撃者はこの問題を不正利用して生成されたキーを推測し、設定された IP 制約と一致させます。不正利用により、攻撃者が *ntpdc* クエリまたはコンフィギュレーション リクエストを送信する可能性があります。

  この問題には CVE ID として CVE-2014-9293 が割り当てられています。

  Cisco Product Security Incident Response Team（PSIRT）は、これは脆弱性ではなく、堅牢化に関する問題と考えています。

- ntp-keygen が弱いシードを持つ非暗号乱数生成器を使用して対称キーを生成

- *ntpd* の *ntp-keygen* の問題によって、認証されていないリモートの攻撃者が生成された MD5 キーの推測に成功する可能性があります。

  この問題の原因は *ntp-keygen* が MD5 キーの生成に脆弱なメソッドを使用していることです。攻撃者は生成された MD5 キーを推測することでこの問題を不正利用できる可能性があります。不正利用により、攻撃者は推測した MD5 キーを使用して、信頼できる NTP クライアントまたはサーバになりすます可能性があります。

  この問題には CVE ID として CVE-2014-9294 が割り当てられています。

  Cisco PSIRT は、これは脆弱性ではなく、堅牢化に関する問題と考えています。

- ntpd に存在する複数のバッファ オーバーフローの脆弱性
- *ntpd* の *crypto_recv()*、*ctl_putdata()*、および *configure()* に脆弱性が存在するため、認証されていないリモートの攻撃者がスタック バッファ オーバーフローを引き起こし、続けて *ntpd* プロセスの特権レベルで悪意あるコードを実行する可能性があります。

  この脆弱性は、受信したパケットの検証チェックが不正確であることに起因します。攻撃者は巧妙に細工したリクエスト パケットを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は *ntpd* プロセスを破壊する可能性があります。また、*ntpd* プロセスの特権レベルで任意のコードを実行する可能性もあります。

  この脆弱性には CVE ID として CVE-2014-9295 が割り当てられています。

- ntpd receive()：エラー時の Return の欠落
- 特定の稀なエラーが発生した際、*ntp* の *ntp_proto.c:receive()* コード パスでのエラー検知の問題により処理が停止しない可能性があります。

  この問題は、エラーが検出された際のコード パスに *return;* がないことに起因します。攻撃者がこの問題をどのように不正利用できるかはまだわかっていません。該当システムへの影響も不明です。

  この問題には CVE ID として CVE-2014-9296 が割り当てられています。

  Cisco PSIRT は、現段階ではこれを脆弱性とは考えていません。

- NTP ntp_crypto.c での不適切な検証の脆弱性
- A この脆弱性は *ntpd* の *ntp_crypto.c* に存在し、認証されていないリモートの攻撃者が重要な情報を取得できる可能性があります。

  この脆弱性は *vallen* の不適切な検証によるものです。攻撃者は *ntpd* が稼働し、脆弱な自動鍵認証が設定されているデバイスへ不正なパケットを送信することでこの脆弱性を悪用し、重要な情報が取得される可能性があります。

  この問題には CVE ID として CVE ID CVE-2014-9297 が割り当てられています。

- NTP IPv6 ACL バイパスの脆弱性

- IPv6 アドレスの取り扱いに関する脆弱性により、 認証されていないリモートの攻撃者が脆弱なシステムへ ソース アドレス **::1** に偽装した IPv6 パケットを送信出来る可能性があります。

  この脆弱性は不適切な IPv6 アドレスの処理によるものです。攻撃者は影響を受けるホストへソース アドレス **::1** を用いて IPv6 パケットを送信することでこの脆弱性を悪用でき、IPv6 ソース アドレスに基づいた アプリケーション ACL をバイパスできるようになります。

  この問題には CVE ID として CVE-2014-9298 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでのバッファ オーバーフローの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

Multiple Buffer Overflow Vulnerabilities in ntpd **Calculate the environmental score of**					
CVSS Base Score - **7.5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Partial
CVSS Temporal Score - **7.1**					
Exploitability		Remediation Level		Report Confidence	
Functional		Unavailable		Confirmed	

NTP ntp_crypto.c Improper Validation Vulnerability Calculate the environmental score of .					
CVSS Base Score - **4.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
{INSERT VECTOR}	Medium	None	Partial	None	None
CVSS Temporal Score - **4.1**					
Exploitability		Remediation Level		Report Confidence	
Functional		Unavailable		Confirmed	

NTP IPv6 ACL Bypass Vulnerability Calculate the environmental score of .					
CVSS Base Score - **5.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	None	None
CVSS Temporal Score - **4.5**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Unavailable		Confirmed	

影響

この脆弱性の不正利用に成功した場合、攻撃者は該当デバイス上で任意のコードを実行したり、DoS 状態を発生させたりできる可能性があります。

NTP ntp_crypto.c での不適切な検証の脆弱性の不正利用に成功した場合、情報漏洩の可能性があります。

NTP IPv6 ACL バイパスの脆弱性不正利用に成功した場合の *ntpd* の **restrict** コマンドが回避される可能性があります。

ソフトウェア バージョンおよび修正

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

このセクションは、各製品の調査が終了したときに記入されます。

回避策

デバイスが NTP コントロール クエリーの処理を行わないようにすることが対応策になります。ntp.conf の編集が可能な製品では、これは **restrict** ディレクティブによって実現できます。他の製品では **ntp access-group** がサポートされ、NTP コントロール クエリーをフィルタできる場合があります。それぞれの影響を受ける製品での回避策については各 Cisco Bug ID の workaround セクションを参照してください。

ネットワーク内のシスコデバイスに導入できる対応策については、このアドバイザリの付属ドキュメント『Cisco Applied Intelligence』を参照してください。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=36857

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレードを入手することができます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、E メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

不正利用事例と公式発表

Cisco 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。

これらの脆弱性は、US-CERT/CC からシスコに報告されました。

この通知のステータス：Final

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。新しい情報が入り次第、このドキュメントは更新される予定です。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141222-ntpd

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org

- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- fulldisclosure@seclists.org

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

今後のドキュメントや関連コンテンツの入手手順については、Security Vulnerability Policy ページの Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 2.10	2015-March-31	Updated the First Fixed Software.
Revision 2.9	2015-March-26	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Moved Cisco IP Interoperability and Collaboration System (IPICS) from affected to not vulnerable for CVE-2014-9297, CVE-2014-9298.
Revision 2.8	2015-March-11	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 2.7	2015-March-04	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 2.6	2015-March-03	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 2.5	2015-February-23	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 2.4	2015-February-18	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 2.3	2015-February-18	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev	2015-	Updated the Affected Products,

isio n 2.2	February-16	Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 2.1	2015-February-12	Cisco UCS Manager, Virtual Systems Operations Center for vPE project, and Cisco TelePresence Manager (CTSMan) were moved from Vulnerable to Not Vulnerable.
Rev isio n 2.0	2015-February-11	Added the two new CVE IDs from ntp.org. Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Note: Cisco WebEx Meeting Server versions 2.x moved from Vulnerable to Not Vulnerable. Cisco Business Edition 3000 (BE3k) removed from advisory as end of life.
Rev isio n 1.1 7	2015-February-03	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Note: Cisco Videoscape Conductor moved from Not Vulnerable to Vulnerable
Rev isio n 1.1 6	2015-January-27	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Moved Cisco TelePresence Exchange System (CTX) and Cisco Unified SIP Proxy from Vulnerable section to Not Vulnerable.
Rev isio n 1.1 5	2015-January-26	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Cisco TelePresence ISDN Link moved from Vulnerable to Not Vulnerable.
Rev isio n 1.1 4	2015-January-21	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.1 3	2015-January-16	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.1 2	2015-January-15	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev	2015-	Updated the Affected Products,

isio n 1.1 1	January-13	Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.1 0	2015-January-12	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.9	2015-January-09	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.8	2015-January-08	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.7	2015-January-07	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.6	2015-January-06	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.5	2014-Decembe r-31	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.4	2014-Decembe r-26	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.3	2014-Decembe r-26	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.2	2014-Decembe r-24	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Rev isio n 1.1	2014-Decembe r-23	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.Added AMB Publication link in Workarounds Section.
Rev isio n 1.0	2014-Decembe r-22	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、Cisco Security Advisory に関してメディアが問い合わせる際の指示が掲載されています。すべての Cisco Security Advisory は、http://www.cisco.com/go/psirt/ で確認することができます。

Cisco Security Advisories
Cisco Intrusion Prevention System Signatures
Cisco Applied Mitigation Bulletins
Cisco Security Blog
Cisco Event Response Pages
Cisco IntelliShield Alerts
Cisco Security Notices
Cisco Security Responses
Cisco Cyber Risk Reports
Cisco Security White Papers
Snort Rules