Cisco Security Advisory

Multiple Vulnerabilities in ntpd Affecting Cisco Products

High

Advisory ID: cisco-sa-20141222-ntpd
Last Updated: 2015 March 31 15:29 GMT
Published: 2014 December 22 16:00 GMT
Version2.10: Final
CVSS Score: Base - 7.5
Workarounds: See below
Cisco Bug IDs: CSCus26858 CSCus26864 CSCus26870 CSCus26875 CSCus26882 CSCus26891 CSCus26895 CSCus26946 CSCus26947 CSCus26956 CSCus27007 CSCus27224 CSCus27225 CSCus27226 CSCus27229 CSCus27239 CSCus27240 CSCus27241 CSCus27243 CSCus27244 CSCus27245 CSCus27246 CSCus27247 CSCus27248 CSCus27253 CSCus27274 CSCus27279 CSCus27280 CSCus27283 CSCus27291 CSCus27292 CSCus27295 CSCus27309 CSCus27325 CSCus27337 CSCus27369 CSCus27388 CSCus27391 CSCus27395 CSCus27413 CSCus27416 CSCus27423 CSCus27483 CSCus27501 CSCus27527 CSCus27577 CSCus27589 CSCus29415 CSCus30138 CSCus43427 CSCus82092 CSCus83811 CSCus88284 CSCus88292 CSCus88487 CSCus90552 CSCus90674 CSCus90733

CVE-2014-9293
CVE-2014-9294
CVE-2014-9295
CVE-2014-9296
CVE-2014-9297
CVE-2014-9298
CWE-119
CWE-20
CWE-200
CWE-264
CWE-310

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

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

Related Resources

AMB Identifying and Mitigating Multiple Vulnerabilities in Network Time Protocol

ST 32890

Subscribe to Cisco Security Notifications

Subscribe

Summary

Multiple Cisco products incorporate a version of the *ntpd* package. Versions of this package are affected by one or more vulnerabilities that could allow an unauthenticated, remote attacker to execute arbitrary code or create a denial of service (DoS) condition.

On December 19, 2014, NTP.org and US-CERT released security advisories detailing two issues regarding weak cryptographic pseudorandom number generation (PRNG), three buffer overflow vulnerabilities, and an unhandled error condition with an unknown impact. These vulnerabilities are referenced in this document as follows:

- CVE-2014-9293: Weak Default Key in config_auth()
- CVE-2014-9294: Noncryptographic Random Number Generator with Weak Seed Used by ntp-keygen to Generate Symmetric Keys
- CVE-2014-9295: Multiple Buffer Overflow Vulnerabilities in ntpd
- CVE-2014-9296: ntpd receive(): Missing Return on Error

On February 4, 2015, NTP.org and US-CERT released two additional vulnerabilities regarding improper validation of *vallen* in *ntp_crypto.c* and an IPv6 ::1 ACL bypass vulnerability. These vulnerabilities were added to their original advisory. For completeness, these vulnerabilities are referenced in this document as follows:

- CVE-2014-9297: NTP ntp_crypto.c Improper Validation Vulnerability
- CVE-2014-9298: NTP IPv6 ACL Bypass Vulnerability

This advisory will be updated as additional information becomes available.

Cisco will release software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141222-ntpd

Affected Products

Vulnerable Products

Products and services listed in the following table have had their exposure to CVE-2014-9295 confirmed.

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 5.0.0 to 5.1.0 (5-Apr-2015) Patch file available for Cisco Service Control Engine 8000 Series versions 3.5.0 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

Products and services listed in the following table have had their exposure to CVE-2014-9297 and/or CVE-2014-9298 confirmed.

Product	Defect	Fixed releases availability
Network and Content Security Devices		
Cisco Physical Access Gateway	CSCus27369	1.5(3.0.3.2) (15-April-2015)
Network Management and Provisioning		
Cisco Prime Data Center Network Manager (.ova and .iso installers)	CSCus88284	7.1(2)PF (31-Mar-2015)
Cisco Quantum Policy Suite (QPS)	CSCus27432	7.5 (Available 30-Jun-2015)
Cisco Virtual Systems Operations Center for vPE 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 Heartbeat Server	CSCus89695	SR10 (13-Feb-15) RMS 4.1 (13-Feb-15) RMS 5.0 (13-Feb-15)
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		
Cisco TelePresence Endpoints (C series, EX series, MX series, MXG2 series, SX series) and the 10" touch panel	CSCus88487	7.3.2
Cisco TelePresence TE Software (for E20 - EoL)	CSCus90674	TE 4.1.6 (April 2015)
Cisco Video Delivery System Recorder	CSCus62967	Update via Admin Shell
Cisco Videoscape Back Office (VBO)	CSCus82885	V4.0-Branch (27-Mar-2015)
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

Products Confirmed Not Vulnerable

Not Vulnerable to CVE-2014-9297 or CVE-2014-9298

The following Cisco products have been analyzed. While they are affected by CVE-2014-9295, they are not affected by either CVE-2014-9297 or CVE-2014-9298.

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

Not Vulnerable to Any Listed Vulnerabilities

The following Cisco products have been analyzed and are not affected by any of the listed vulnerabilities:

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

This section will continue to be populated when investigation of each product has concluded.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

On December 19, 2014, NTP.org and US-CERT released security advisories for *ntpd* detailing two issues regarding weak cryptographic pseudorandom number generation (PRNG), three buffer overflow vulnerabilities, and an unhandled error condition with an unknown impact. Further, on February 4, 2015, these advisories were updated to include an autokey authentication vulnerability and an IPv6 ACL bypass vulnerability.

The impact of these vulnerabilities on Cisco products may vary depending on the affected product.

For Cisco products, refer to the information provided in the Cisco bug IDs listed in the "Affected Products" section of this document.

Additional information and detailed instructions are available in the Cisco installation, configuration, and maintenance guides for each product. If additional clarification or advice is needed, please contact your support organization.

The vulnerability names and associated Common Vulnerabilities and Exposures (CVE) IDs are as follows:

- **Weak Default Key in config_auth()**

  An issue in the generation of a random key for *ntpd* could allow an unauthenticated, remote attacker to guess the generated key. The attacker may be able to use it to send *ntpdc* query or configuration requests.

  The issue occurs because *ntpd* automatically generates weak keys if no *ntpdc* request authentication key was specified in the *ntp.conf* configuration file. An attacker could exploit this issue by guessing the generated key and matching any configured IP restrictions. An exploit could allow the attacker to send *ntpdc* query or configuration requests.

  This issue has been assigned CVE ID CVE-2014-9293.

  The Cisco Product Security Incident Response Team (PSIRT) considers this a hardening issue rather than a vulnerability.

- **Noncryptographic Random Number Generator with Weak Seed Used by ntp-keygen to Generate Symmetric Keys**

An issue in *ntp-keygen* of *ntpd* could allow an unauthenticated, remote attacker to guess the generated MD5 keys.

The issue occurs because *ntp-keygen* uses a weak method for generating the MD5 keys. An attacker could exploit this issue by guessing the generated MD5 keys. An exploit could allow the attacker to use the guessed MD5 keys to spoof a trusted NTP client or server.

This issue has been assigned CVE ID CVE-2014-9294.

Cisco PSIRT considers this a hardening issue rather than a vulnerability.

- **Multiple Buffer Overflow Vulnerabilities in ntpd**

  Vulnerabilities in *crypto_recv(), ctl_putdata(),* and *configure()* of *ntpd* could allow an unauthenticated, remote attacker to cause a stack buffer overflow, which could allow the attacker to execute malicious code with the privilege level of the *ntpd* process.

  The vulnerabilities are due to incorrect validation checks on the received packets. An attacker could exploit these vulnerabilities by sending crafted request packets. An exploit could allow the attacker to crash the *ntpd* process. Arbitrary code execution with the privilege level of the *ntpd* process may also be possible.

  This vulnerability has been assigned CVE ID CVE-2014-9295.

- **ntpd receive(): Missing Return on Error**

  An issue in *ntp_proto.c:receive()* of *ntp* in the code path where an error was detected could indicate processing did not stop when a specific rare error occurs.

  The issue is due to a missing *return;* in the code path where an error was detected. It has not been proven how an attacker could exploit this issue. The impact to the affected system is also unknown.

  This issue has been assigned CVE ID CVE-2014-9296.

  Cisco PSIRT at this stage does not consider this to be a vulnerability.

- **NTP ntp_crypto.c Improper Validation Vulnerability**

  A vulnerability in *ntp_crypto.c* of *ntpd* could allow an unauthenticated, remote attacker to obtain sensitive information.

  The vulnerability is due to improper validation of *vallen*. An attacker could exploit this vulnerability by sending crafted packets to a device running *ntpd* and configured with autokey authentication. An exploit could allow the attacker to retrieve sensitive information.

  This issue has been assigned CVE ID CVE-2014-9297.

- **NTP IPv6 ACL Bypass Vulnerability**

  A vulnerability in IPv6 address handling could allow an unauthenticated, remote attacker to send IPv6 network packets to a vulnerable system using a spoofed source address of ::1 on an interface not configured for localhost.

  The vulnerability is due to improper IPv6 address processing. An attacker could exploit this issue by sending IPv6 packets with a source address of ::1 to an affected host. An exploit could allow the attacker to bypass application ACLs that rely on IPv6 source address filtering.

  This issue has been assigned CVE ID CVE-2014-9298

Workarounds

Mitigations involve preventing the device from processing NTP control queries. In products that allow for editing the ntp.conf file, this is accomplished by the **restrict** directive. Other products may support **ntp access-group** commands which can be used to filter NTP control queries. Potential workarounds for each affected Cisco product is referenced in the Cisco Bug ID workarounds section.

Mitigations that can be deployed on Cisco devices in a network are available in the Cisco Applied Intelligence companion document for this advisory:
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=36857

Fixed Software

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

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

This section will be populated when investigation of each product has concluded.

Exploitation and Public Announcements

Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

These vulnerabilities were reported to Cisco by US-CERT/CC.

URL

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

---

Revision History

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.
Revision 2.2	2015-February-16	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 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.
Revision 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.

Revision 1.17	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
Revision 1.16	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.
Revision 1.15	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.
Revision 1.14	2015-January-21	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.13	2015-January-16	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.12	2015-January-15	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.11	2015-January-13	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.10	2015-January-12	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.9	2015-January-09	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.8	2015-January-08	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.7	2015-January-07	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, and Workaround sections.
Revision 1.6	2015-January-06	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.5	2014-December-31	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.4	2014-December-30	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.3	2014-December-26	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.2	2014-December-24	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.1	2014-December-23	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Added AMB publication link in Workarounds section.
Revision 1.0	2014-December-22	Initial public release.