Cisco Security Advisory

OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products

Advisory ID:	cisco-sa-20140409-heartbleed
Last Updated:	2014 October 29 16:11 GMT
Published:	2014 April 9 03:00 GMT
Version1.26:	Interim
CVSS Score:	Base - 5.0
Workarounds:	See below
Cisco Bug IDs:	CSCuo17488

CVE-2014-0160
CWE-200

Download CVRF

Download PDF

Email

Summary

Multiple Cisco products incorporate a version of the OpenSSL package affected by a vulnerability that could allow an unauthenticated, remote attacker to retrieve memory in chunks of 64 kilobytes from a connected client or server.

The vulnerability is due to a missing bounds check in the handling of the Transport Layer Security (TLS) heartbeat extension. An attacker could exploit this vulnerability by implementing a malicious TLS or Datagram Transport Layer Security (DTLS) client, if trying to exploit the vulnerability on an affected server, or a malicious TLS or DTLS server, if trying to exploit the vulnerability on an affected client. An exploit could send a specially crafted TLS or DTLS heartbeat packet to the connected client or server. An exploit could allow the attacker to disclose a limited portion of memory from a connected client or server for every heartbeat packet sent. The disclosed portions of memory could contain sensitive information that may include private keys and passwords.

Please note that the devices that are affected by this vulnerability are the devices acting as an SSL server terminating SSL connections or devices acting as an SSL Client initiating an SSL connection. Devices that are simply traversed by SSL traffic without terminating it are not affected.

This advisory will be updated as additional information becomes available. Cisco will release software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities may be available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

Affected Products

Cisco is currently investigating its product line to determine which products may be affected by this vulnerability and the impact on the affected product.

The following Cisco products are currently under investigation:

No Cisco products are currently under investigation.

The following Cisco services are currently under investigation:

No Cisco hosted services are currently under investigation.

Products and services listed in the subsections below have had their exposure to this vulnerability confirmed. Additional products will be added to these sections as the investigation continues.

Vulnerable Products

Customers interested in tracking the progress of any of the following bugs can visit the Cisco Bug Search Tool to view the defect details and optionally select *Save Bug* and activate the *Email Notification* feature to receive automatic notifications when the bug is updated.

The following Cisco products are affected by this vulnerability:

- Cisco Agent for OpenFlow [CSCuo30098]
- Cisco AnyConnect Secure Mobility Client for iOS [CSCuo17488]
- Cisco ASA CX Context-Aware Security [CSCuo24523]
- Cisco Common Services Platform Collector [CSCuo29151]
- Cisco Desktop Collaboration Experience DX650 [CSCuo16892]
- Cisco Edge 340 Digital Media Player [CSCuo24301]
- Cisco Expressway Series [CSCuo16472]
- Cisco FireAMP Private Cloud virtual appliance
- Cisco IOS XE [CSCuo19730]
- Cisco Cisco Internet Streamer CDS [CSCuo31566]
- Cisco Jabber Video for TelePresence (Movi) [CSCuo28855]
- Cisco MATE Products [CSCuo22177]
- Cisco Mobility Service Engine (MSE) [CSCuo20622]
- Cisco MS200X Ethernet Access Switch [CSCuo18736]
- Cisco OnePK All-in-One VM [CSCuo19843]
- Cisco ONS 15454 Series Multiservice Provisioning Platforms [CSCuo22921]
- Cisco Prime Collaboration Deployment [CSCuo34385]
- Cisco Prime IP Express [CSCuo35657]
- Cisco Prime License Manager [CSCuo32735]
- Cisco Prime Network Registrar (CPNR) [CSCun82386]
- Cisco Prime Network Services Controller [CSCuo20385]
- Cisco Prime Security Manager [CSCuo27123]
- Cisco Security Manager [CSCuo19265]
- Cisco Small Business ISA500 Series Integrated Security Appliances [CSCuo29778]
- Cisco TelePresence 1310 [CSCuo20210]
- Cisco TelePresence Conductor [CSCuo20306]
- Cisco TelePresence EX Series [CSCuo26378]
- Cisco Telepresence Integrator C Series [CSCuo26378]
- Cisco TelePresence IP Gateway Series [CSCuo21597]
- Cisco TelePresence ISDN GW 3241 [CSCuo21486]
- Cisco TelePresence ISDN GW MSE 8321 [CSCuo21486]
- Cisco TelePresence ISDN Link [CSCuo26686]
- Cisco TelePresence MX Series [CSCuo26378]
- Cisco TelePresence Profile Series [CSCuo26378]
- Cisco TelePresence Serial Gateway Series [CSCuo21535]
- Cisco TelePresence Server 8710, 7010 [CSCuo21468]
- Cisco TelePresence Server on Multiparty Media 310, 320 [CSCuo21468]
- Cisco TelePresence Server on Virtual Machine [CSCuo21468]
- Cisco TelePresence System 1000 [CSCuo20210]
- Cisco TelePresence System 1100 [CSCuo20210]
- Cisco TelePresence System 1300 [CSCuo20210]
- Cisco TelePresence System 3000 Series [CSCuo20210]
- Cisco TelePresence System 500-32 [CSCuo20210]
- Cisco TelePresence System 500-37 [CSCuo20210]
- Cisco TelePresence Supervisor MSE 8050 [CSCuo21584]
- Cisco TelePresence SX Series [CSCuo26378]
- Cisco TelePresence TX 9000 Series [CSCuo20210] Version 6.1.2.0 and prior
- Cisco TelePresence Video Communication Server (VCS) [CSCuo16472]
- Cisco Unified 7800 Series IP Phones [CSCuo16987]
- Cisco Unified 8961 IP Phone [CSCuo16938]
- Cisco Unified 9951 IP Phone [CSCuo16938]
- Cisco Unified 9971 IP Phone [CSCuo16938]
- Cisco Unified Communications Domain Manager (Cisco Unified CDM) 10.1(1) [CSCur10784]
- Cisco Unified Communications Manager (UCM) 10.0 [CSCuo17440]
- Cisco Unified Communications Manager Session Management Edition (SME) [CSCuo17440]
- Cisco Unified Presence Server (Cisco UPS)[CSCuo21298], [CSCuo21289]
- Cisco Unified Workforce Optimization [CSCuo43820]
- Cisco Unity Connection (UC)[CSCuo30041]
- Cisco Universal Small Cell 5000 Series running V3.4.2.x software [CSCuo22301]
- Cisco Universal Small Cell 7000 Series running V3.4.2.x software [CSCuo22301]
- Cisco Videoscape Conductor [CSCuo46307]
- Cisco Video Distribution Suite for Internet Streaming VDS-IS [CSCuo43012]
- Cisco Video Surveillance 3000 Series IP Cameras [CSCuo37282]
- Cisco Video Surveillance 4000 Series IP Cameras [CSCuo37288]
- Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras [CSCuo37283]
- Cisco Video Surveillance 6000 Series IP Cameras [CSCuo37282]
- Cisco Video Surveillance 7000 Series IP Cameras [CSCuo37282]
- Cisco Video Surveillance PTZ IP Cameras [CSCuo37282]
- Cisco WebEx Meetings for Android [CSCuo20617]
- Cisco WebEx Meetings for Windows Phone 8 [CSCuo32707]
- Cisco WebEx Meetings Server (client) [CSCuo29780]
- Cisco WebEx Meetings Server versions 2.x [CSCuo17528]
- Cisco WebEx Node for ASR 1000 Series [CSCuo33614]
- Cisco WebEx Node for MCS [CSCuo33612]
- Cisco Wireless Location Appliance [CSCuo20622]
- Small Cell factory recovery root filesystem V2.99.4 or later [CSCuo22358]
- Tandberg Codian MSE 8320 model [CSCuo21486]
- Tandberg Codian ISDN GW 3210/3220/3240 [CSCuo21486]

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

SA OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products

BLG OpenSSL Heartbleed Vulnerability CVE-2014-0160 - Cisco Products and Mitigations

BLG Heartbleed: Transparency for Our Customers

BLG Cisco IPS Signature Coverage for OpenSSL Heartbleed Issue

ST 30510

ST 30511

ST 30512

ST 30513

ST 30514

ST 30515

ST 30516

ST 30517

ST 30520

ST 30521

ST 30522

ST 30523

ST 30524

ST 30525

ST 30549

ST 30711

ST 30712

ST 30713

ST 30714

ST 30715

ST 30716

ST 30717

ST 30718

ST 30719

ST 30720

ST 30721

ST 30722

ST 30723

ST 30724

ST 30725

ST 30726

ST 30727

ST 30728

ST 30729

ST 30730

ST 30731

ST 30732

ST 30733

ST 30734

ST 30735

Other Cisco products may be affected by this vulnerability. The list of affected products will be updated as the investigation continues.

For each of the above products listed as Vulnerable, information about the following will be made available on the associated Cisco bug ID:

- Vulnerable and non-vulnerable releases
- First release incorporating the fix
- Workarounds and mitigations (if available)
- Impact assessment per affected product feature

The following Cisco hosted services are affected by this vulnerability:

No Cisco hosted services are currently known to be affected.

The following Cisco hosted services were previously identified as vulnerable and have been remediated:

- Cisco Registered Envelope Service (CRES) [CSCuo16974] [CSCuo17116]
- Cisco USC Invicta Series Autosupport Portal
- Cisco Webex Messenger Service

Products Confirmed Not Vulnerable

NOTE: the following list includes Cisco applications that are intended to be installed on a customer-provided host (either a physical server or a virtual machine) with a customer-installed operating systems. Those products may use the Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) functionality as provided by the host operating system on which the Cisco product is installed. While those Cisco products do not directly include an affected version of openssl (and hence they are not impacted by this vulnerability), Cisco recommends customers to review their host operating system installation and perform any upgrades necessary to address this vulnerability, according to the operating system vendor recommendations and general operating system security best practices.

The following Cisco products have been analyzed and are not affected by this vulnerability:

- Cisco 1000 Series Connected Grid Routers
- Cisco 200 Series Smart Switches
- Cisco 300 Series Managed Switches
- Cisco 500 Series Stackable Managed Switches
- Cisco ACE Application Control Engine Appliance
- Cisco ACE Application Control Engine Module (ACE10, ACE20, ACE30)
- Cisco ACE Global Site Selector Appliances (GSS)
- Cisco Adaptive Security Appliance (ASA) Software
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco Agent Desktop
- Cisco Anomaly Guard Module
- Cisco AnyConnect Secure Mobility Client for Android
- Cisco AnyConnect Secure Mobility Client for desktop platforms
- Cisco Application and Content Networking System (ACNS) Software
- Cisco Application Networking Manager (ANM)
- Cisco ASR 5000 Series
- Cisco ATA 187 Analog Telephone Adapter
- Cisco Broadband Access Center Telco Wireless
- Cisco Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module (FWSM)
- Cisco Catalyst Operating System (CatOS)
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco Configuration Professional
- Cisco Connected Grid Device Manager
- Cisco Connected Grid Network Management System
- Cisco Content Security Management Appliance (SMA)
- Cisco Content Switching Module with SSL (CSM-S)
- Cisco CSS 11500 Series Content Services Switches
- Cisco CVR100W Wireless-N VPN Router
- Cisco D9034-S Encoder
- Cisco D9036 Modular Encoding Platform
- Cisco D9054 HDTV Encoder
- Cisco D9804 Multiple Transport Receiver
- Cisco D9824 Advanced Multi Decryption Receiver
- Cisco D9854/D9854-I Advanced Program Receiver
- Cisco D9858 Advanced Receiver Transcoder
- Cisco D9859 Advanced Receiver Transcoder
- Cisco D9865 Satellite Receiver
- Cisco DCM Series D9900 Digital Content Manager
- Cisco Digital Media Manager (DMM)
- Cisco Digital Media Players
- Cisco DPC/EPC 2202 VoIP Cable Modem
- Cisco DPC/EPC 2203 VoIP Cable Modem
- Cisco DPC/EPC 3208 VoIP Cable Modem
- Cisco DPC/EPC2100 Cable Modem
- Cisco DPC/EPC2325 Residential Gateway with Wireless Access Point
- Cisco DPC/EPC2425 Wireless Residential Gateway with Embedded Digital Voice Adapter
- Cisco DPC/EPC2434 VoIP Wireless Home Gateway
- Cisco DPC/EPC2505 Cable Modem
- Cisco DPC/EPC2607 Cable Modem
- Cisco DPC/EPC3010 Cable Modem
- Cisco DPC/EPC3212 VoIP Cable Modem
- Cisco DPC2320 and EPC2320 Wireless Residential Gateway
- Cisco DPC2325R2 and EPC2325R2 Wireless Residential Gateway
- Cisco DPC2420 and EPC2420 Wireless Residential Gateway with Embedded Digital Voice Adapter
- Cisco DPC3000/EPC3000 Cable Modem
- Cisco DPC3008/EPC3008 Cable Modem
- Cisco DPC3825 and EPC3825 8x4 DOCSIS 3.0 Wireless Residential Gateway
- Cisco DPC3827 and EPC3827 Wireless Residential Gateway
- Cisco DPC3828 and EPC3828 DOCSIS/EuroDOCSIS 3.0 8x4 Wireless Residential Gateway
- Cisco DPC3925 and EPC3925 8x4 DOCSIS 3.0 Wireless Residential Gateway with EDVA
- Cisco DPC3928 and EPC3928 DOCSIS/EuroDOCSIS 3.0 8x4 Wireless Residential Gateway with Embedded Digital Voice Adapter
- Cisco DPC3939 DOCSIS 3.0 16x4 Wireless Residential Voice Gateway
- Cisco DPQ/EPQ2160 DOCSIS 2.0 Cable Modem
- Cisco DPQ2202 VoIP Cable Modem
- Cisco DPQ2425 Wireless Residential Gateway with Digital Voice Adapter
- Cisco DPQ3212 VoIP Cable Modem
- Cisco DPQ3925 8x4 DOCSIS 3.0 Wireless Residential Gateway with EDVA
- Cisco DPR/EPR2320, DPR2325 Cable Modem with Wireless Access Point
- Cisco DPR362 Cable Modem and Router
- Cisco DPX/EPX 2203 VoIP Cable Modem
- Cisco DPX/EPX 2203C VoIP Cable Modem
- Cisco DPX/EPX2100 Cable Modem
- Cisco DPX100/120 Cable Modem
- Cisco DPX110 Cable Modem
- Cisco DPX130 Cable Modem
- Cisco DPX213 VoIP Cable Modem
- Cisco DPX2213 VoIP Cable Modem
- Cisco Edge 300 Digital Media Player
- Cisco Email Security Appliance (ESA)
- Cisco Emergency Responder (CER)
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco ESW2 Series Advanced Switches
- Cisco Extensible Network Controller (XNC)
- Cisco Finesse
- Cisco Identity Service Engine (ISE)
- Cisco Insight Reporter
- Cisco Integrated Management Controller (IMC)
- Cisco Intelligent Automation for Cloud
- Cisco IOS XR
- Cisco IOS
- Cisco IP Communicator
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco IP Video Phone E20
- Cisco IPS
- Cisco IronPort Encryption Appliance (IEA)
- Cisco Jabber for Android
- Cisco Jabber for iOS
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco Jabber Software Development Kit
- Cisco Jabber Video for iPad
- Cisco Jabber Voice for Android
- Cisco Jabber Voice for iPhone
- Cisco Linear Stream Manager
- Cisco MDS Switches
- Cisco MediaSense
- Cisco Meraki Cloud-Managed Indoor Access Points
- Cisco Meraki Cloud-Managed Outdoor Access Points

ST 30736
ST 30737
ST 30738
ST 30739
ST 30740
ST 30741
ST 30742
ST 30777
ST 30778
ST 30779
ST 30780
ST 30781
ST 30782
ST 30783
ST 30784
ST 30785
ST 30786
ST 30787
ST 30788
Show All 63...
Subscribe to Cisco Security Notifications
Subscribe

- Cisco Meraki MS Access Switches
- Cisco Meraki MX Security Appliances
- Cisco Mobile Wireless Transport Manager
- Cisco Model DPC2420R2 and EPC2420R2 Wireless Residential Gateway with Digital Voice
- Cisco Model DPC2425R2 and EPC2425R2 Wireless Residential Gateway with Digital Voice
- Cisco Multicast Manager
- Cisco MXE 3500 Series
- Cisco MXE 5600 Series
- Cisco NAC Agent (Clean Access) for Mac
- Cisco NAC Agent (Clean Access) for Web
- Cisco NAC Agent (Clean Access) for Windows
- Cisco NAC Appliance
- Cisco NAC Guest Server
- Cisco NAC Manager
- Cisco NetFlow Generation 3000 Series Appliance
- Cisco Nexus 1000V Switch for Microsoft Hyper-V
- Cisco Nexus 1000V Switch for VMware vSphere
- Cisco Nexus 1010 Virtual Services Appliance
- Cisco Nexus 1100 Virtual Services Appliances
- Cisco Nexus 2000 Series Fabric Extenders
- 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 ONS 15100 Series
- Cisco ONS 15200 Series DWDM Systems
- Cisco ONS 15300 Series
- Cisco ONS 15500 Series
- Cisco ONS 15600 Series
- Cisco ONS 15800 Series DWDM Platforms
- Cisco Packaged Contact Center Enterprise
- Cisco Paging Server
- Cisco Physical Access Gateways
- Cisco Physical Access Manager
- Cisco PowerVu D9190 Conditional Access Manager (PCAM)
- Cisco Prime Access Registrar
- Cisco Prime Analytics
- Cisco Prime Assurance Manager
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Manager
- Cisco Prime Collaboration Provisioning
- Cisco Prime Data Center Network Manager (DCNM)
- Cisco Prime Home
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution (LMS)
- Cisco Prime Network
- Cisco Prime Network Analysis Module (NAM)
- Cisco Prime Optical for SPs
- Cisco Prime Performance Manager for SPs
- Cisco Prime Provisioning for SPs
- Cisco Quantum Policy Suite (QPS)
- Cisco Quantum SON Suite
- Cisco Quantum Virtualized Packet Core
- Cisco Remote Silent Monitoring
- Cisco RV016 VPN Router
- Cisco RV042 VPN Router
- Cisco RV082 VPN Router
- Cisco RV110W Wireless-N VPN Router
- Cisco RV120W Wireless-N VPN Router
- Cisco RV180 VPN Router
- Cisco RV180W Wireless-N VPN Router
- Cisco RV215W Wireless-N VPN Router
- Cisco RV220W Wireless-N VPN Router
- Cisco RV315W Wireless-N VPN Router
- Cisco RV320 VPN Router
- Cisco RV325 VPN Router
- Cisco SCE 8000 Series Service Control Engine
- Cisco SCE 2000 Series Service Control Engine
- Cisco SCE 1000 Series Service Control Engine
- Cisco Secure Access Control Server (ACS)
- Cisco Service Control Subscriber Manager
- Cisco Service Control Collection Manager
- Cisco Service Control Application for Broadband
- Cisco Show and Share (SnS)
- Cisco SocialMiner
- Cisco SourceFire appliances (this includes both 3D Systems and SSL appliances)
- Cisco SSL Services Module (SSLM)
- Cisco TelePresence Advanced Media Gateway Series
- Cisco TelePresence Content Server (TCS)
- Cisco TelePresence Exchange System (CTX)
- Cisco TelePresence IP VCR Series
- Cisco TelePresence Management Suite (TMS)
- Cisco TelePresence Management Suite Analytics Extension
- Cisco TelePresence Management Suite Extension for IBM Lotus Notes
- Cisco TelePresence Management Suite Extension for Microsoft Exchange
- Cisco TelePresence Management Suite Network Integration Extension
- Cisco TelePresence Management Suite Provisioning Extension
- Cisco TelePresence Manager (CTSMan)
- Cisco TelePresence MCU (all series)
- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence MXP Series
- Cisco TelePresence Recording Server (CTRS)
- Cisco Traffic Anomaly Detector
- Cisco UC Integration for IBM Sametime
- Cisco UC Integration for Microsoft Lync
- Cisco UC Integration for Microsoft Office Communicator
- Cisco UCS B-Series (Blade) Servers
- Cisco UCS C-Series (Standalone Rack) Servers
- Cisco UCS Central
- Cisco UCS Fabric Interconnects
- Cisco UCS Invicta Series Solid State Systems
- Cisco Unified 3900 Series IP Phones
- Cisco Unified 6900 Series IP Phones
- Cisco Unified 7900 Series IP Phones
- Cisco Unified 8941 IP Phone
- Cisco Unified 8945 IP Phone
- Cisco Unified Attendant Console (all editions)
- Cisco Unified Attendant Console Advanced
- Cisco Unified Client Services Framework
- Cisco Unified Communications 500 Series
- Cisco Unified Communications Domain Manager (CUCDM) 8.1.4 and earlier
- Cisco Unified Communications Manager (UCM) 9.1(2) and earlier
- Cisco Unified Communications Widgets Click To Call
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco Unified Customer Voice Portal (CVP)
- Cisco Unified Department Attendant Console
- Cisco Unified E-Mail Interaction Manager (EIM)
- Cisco Unified Enterprise Attendant Console
- Cisco Unified Intelligence Center
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified IP Conference Phone 8831
- Cisco Unified Meeting Place Application Server and Web Server
- Cisco Unified Mobility
- Cisco Unified Operations Manager
- Cisco Unified Personal Communicator
- Cisco Unified Provisioning Manager (CUPM)
- Cisco Unified Quick Connect
- Cisco Unified Service Monitor
- Cisco Unified Service Statistics Manager
- Cisco Unified Sip Proxy
- Cisco Unified Video Advantage
- Cisco Unified Web Interaction Manager (WIM)
- Cisco Video Surveillance Media Server Software
- Cisco Video Surveillance Operations Manager Software
- Cisco Videoscape AnyRes Live (CAL)
- Cisco Videoscape AnyRes VOD (CAV)
- Cisco Virtual Network Management Center
- Cisco Virtualization Experience Media Engine
- Cisco Virtual Security Gateway for Microsoft Hyper-V

- Cisco Virtual Security Gateway for VMware
- Cisco VPN Client
- Cisco WAG310G Wireless-G ADSL2+ Gateway with VoIP
- Cisco WAP121 Wireless-N Access Point
- Cisco WAP321 Wireless Access Point
- Cisco WAP4410N Wireless-N Access Point
- Cisco WAP551/561 Wireless-N Access Point
- Cisco Web Security Appliance (WSA)
- Cisco WebEx Connect Client for Windows
- Cisco WebEx Meetings for BlackBerry
- Cisco WebEx Meetings Server versions 1.x
- Cisco WebEx Productivity Tools
- Cisco WebEx Social
- Cisco Wide Area Application Services (WAAS)
- Cisco Wide Area Application Services (WAAS) Express (IOS)
- Cisco Wide Area Application Services (WAAS) Mobile
- Cisco Wireless Control System (WCS)
- Cisco Wireless Lan Controller (WLC)
- CiscoWorks Network Compliance Manager
- CiscoWorks Wireless LAN Solution Engine (WLSE)
- Tandberg 770/880/990 MXP Series

The following Cisco hosted services have been analyzed and are not affected by this vulnerability:

- Cisco Cloud Web Security
- Cisco Meraki Dashboard
- Cisco Partner Support Services
- Cisco Proactive Network Operations Center
- Cisco Smart Call Home
- Cisco Smart Care
- Cisco Smart Net Total Care (SNTC)
- Cisco Smart Services Capabilities
- Cisco Universal Small Cell CloudBase
- Cisco WebEx Event Center
- Cisco WebEx Meeting Center
- Cisco WebEx Support Center
- Cisco WebEx Training Center
- Cisco WebEx WebOffice

Details

A vulnerability in the Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) heartbeat functionality in OpenSSL used in multiple Cisco products could allow an unauthenticated, remote attacker to retrieve memory in chunks of 64 kilobytes from a connected client or server.

The vulnerability is due to a missing bounds check in the handling of the TLS heartbeat extension. An attacker could exploit this vulnerability by implementing a malicious TLS or DTLS client, if trying to exploit the vulnerability on an affected server, or a malicious TLS or DTLS server, if trying to exploit the vulnerability on an affected client. The attacker could then send a specially-crafted TLS or DTLS heartbeat packet to the connected client or server. An exploit could allow the attacker to disclose a limited portion of memory from a connected client or server for every heartbeat packet sent. The disclosed portions of memory could contain sensitive information that may include private keys and passwords.

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2014-0160

**The criteria used to establish whether a Cisco product or service is vulnerable is solely whether it relies on an affected version of the OpenSSL library in order to implement a TLS/DTLS client or server. The criteria does not restrict the analysis to any specific set of protocols that the client or server may implement (eg: HTTPS, SMTP, EAP, etc.).
Based on this criteria the products that are listed in this security advisory as not vulnerable are such no matter which attack vector an attacker may attempt to use to exploit Heartbleed.**

The Cupid attack exploits the Heartbleed bug using the EAP protocol as an attack vector to target the TLS layer in EAP-TLS. The products that are listed in this security advisory that are not vulnerable to the Heartbleed vulnerability are also unaffected by the Cupid attack.

The impact of this vulnerability on Cisco products may vary depending on the affected product.

Given the unique characteristics of the Heartbleed vulnerability, Cisco recommends customers to generate new public/private key pairs, obtain a new certificate for that key pair, and install the new certificate and associated key pair as appropriate on all affected deployments after installing the software updates. This is general advice appropriate for Cisco and non-Cisco devices.

For Cisco products, please refer to the information provided in the Cisco bug IDs, listed in the Affected Products section of this document. Additional information and detailed instructions on how to perform those tasks are available on the Cisco installation, configuration and maintenance guides for each product. If additional clarification or advice is needed, please contact your support organization.

Product Specific Information

Cisco Meraki

> **Cisco has made available additional information in the following document:**
> **https://meraki.cisco.com/blog/2014/04/openssl-and-the-heartbleed-vulnerability/**

Small Cell factory recovery root filesystem

> **The following products leverage the Small cell factory recovery root filesystem V2.99.4 or later. The factory recovery root filesystem is not stored in flash but is downloaded from Cisco USC CloudBase and only used for the duration of the activation/recovery process. OpenSSL is called by the cURL application, which is itself called from a shell script so a malicious user would have no exposure to any Cisco proprietary code and the memory space of the cURL process would not contain any private keys:**

- **DPH-SO16 (Cisco, formerly Ubiquisys)**
- **FAPE-HSP-5620 (OEM)**
- **FAPO-HSP-5900 (OEM)**
- **FAPR-HSP-5110 (OEM)**
- **FC1020 (Cisco, formerly Ubiquisys)**
- **FC1021 (Cisco, formerly Ubiquisys)**
- **FC1022 (Cisco, formerly Ubiquisys)**
- **FC1060 (Cisco, formerly Ubiquisys)**
- **FC1080 (Cisco, formerly Ubiquisys)**
- **FC170U (Cisco, formerly Ubiquisys)**
- **FC173U (Cisco, formerly Ubiquisys)**
- **FC233U (Cisco, formerly Ubiquisys)**
- **FC235U (Cisco, formerly Ubiquisys)**
- **FC270U (Cisco, formerly Ubiquisys)**
- **FEMTO-G3 (Cisco, formerly Ubiquisys)**
- **FEMTOAP-SR1 (Cisco, formerly Ubiquisys)**
- **FEMTOAP-SR2 (Cisco, formerly Ubiquisys)**
- **FMA16301T (OEM)**
- **FP16201 (OEM)**
- **FP8101 (OEM)**
- **FP8131T (OEM)**
- **FPA16241T (OEM)**
- **FPLUS2 (Cisco, formerly Ubiquisys)**
- **G5 (Cisco, formerly Ubiquisys)**
- **G6 (Cisco, formerly Ubiquisys)**
- **S2000 (OEM)**
- **SH170U (Cisco, formerly Ubiquisys)**
- **SH173U (Cisco, formerly Ubiquisys)**
- **USC3331 (Cisco)**
- **USC5310 (Cisco)**
- **USC5330 (Cisco)**
- **USC7330 (Cisco)**
- **USC9330 (Cisco)**
- **ZM-000-05-0005 (Cisco, formerly Ubiquisys)**
- **ZP-000-05EU-0004 (Cisco, formerly Ubiquisys)**
- **ZP-000-07EU-0001 (Cisco, formerly Ubiquisys)**
- **ZP-001-03EU-0003 (Cisco, formerly Ubiquisys)**
- **ZP-001-03EU-0005 (Cisco, formerly Ubiquisys)**
- **ZP-001-03EU-0006 (Cisco, formerly Ubiquisys)**
- **ZP-005-02EU-0002 (Cisco, formerly Ubiquisys)**

Cisco Universal Small Cell 5000 Series and Cisco Universal Small Cell 7000 Series

> **A malicious user cannot get the private key of the Universal Small Cell (USC) product as the private keys are held in a separate protected memory space; however, the malicious user may be able to access memory containing the Small Cell internal OM database and configuration details.**

Cisco Collaboration Systems 10.x:

Cisco Unified Communications Manager (UCM) version 10.0, Cisco Unity Connection (UC) version 10.0, and Cisco Unified Presence Server (CUPS) version 10.0 are affected by the OpenSSL vulnerability described in this advisory. An unauthenticated, remote attacker with the ability to open a TCP connection to an affected port may exploit the vulnerability. Successful exploitation may allow the attacker to disclose potentially sensitive information.

Cisco voice and presence devices open a number of service ports to accept connections from users, administrators, phones, and IP voice gateways. A majority of these services are secured utilizing SSL or TLS and may be leveraged by an attacker to exploit the vulnerability.

Cisco Unified IP Phones:

Cisco Unified 7800 Series, Cisco Unified 8961, Cisco Unified 9951, and Cisco Unified 9971 IP Phones may be exposed to the vulnerability when the secure Web Management interface is enabled. Additionally, attacks may be executed via secure SIP and secure RTP.

An unauthenticated, remote attacker with the ability to reach the Web Management interface when enabled, or that can place a direct secure SIP call to the device may trigger the vulnerability. Successful exploitation may allow the attacker to disclose potentially sensitive information.

Voice networks that have been deployed using Cisco Secure Configuration Guidelines are at a reduced risk from outside attackers. Phones that have been segmented from the common use network should restrict the attack surface to other phones and users who have direct access to the voice network.

Cisco Desktop Collaboration Experience:

Cisco Desktop Collaboration Experience DX650 devices may be exposed via the secure Web Management Interface when enabled. These devices may also be exploited via secure SIP, secure RTP, as well as any other application installed on the device that utilizes the system-supplied OpenSSL library.

An unauthenticated, remote attacker with the ability to reach the Web Management interface when enabled can place a direct secure SIP call to the device, or access an affected service may trigger the vulnerability. Successful exploitation may allow the attacker to disclose potentially sensitive information.

Voice networks that have been deployed using Cisco Secure Configuration Guidelines are at a reduced risk from outside attackers. Phones that have been segmented from the common use network should restrict the attack surface to other phones and users who have direct access to the voice network.

Voice Networks Security Hardening Guidelines:

Cisco provides a comprehensive design guide for all voice network deployments. This includes suggested security feature configurations on intermediate and edge devices to prevent spoofed traffic from being passed on the voice network as well as the isolation and segregation of voice traffic from general network traffic. Security information for Cisco Collaboration Systems 10.x is available at the following link:
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab10/collab10/security.html

Cisco AnyConnect Secure Mobility Client for iOS

This vulnerability does not affect the versions of Cisco AnyConnect Secure Mobility Client released for devices running iOS 5 or earlier.

Cisco IOS XE Software

Cisco IOS XE Software Release	First Fixed Release
2.x.x	Not vulnerable
3.1.xS	Not vulnerable
3.1.xSG	Not vulnerable
3.2.xS	Not vulnerable
3.2xSE	Not vulnerable
3.2.xSG	Not vulnerable
3.2.xXO	Not vulnerable
3.2.xSQ	Not vulnerable
3.3.xS	Not vulnerable
3.3.xSE	Not vulnerable
3.3xSG	Not vulnerable
3.3xXO	Not vulnerable
3.3xSQ	Not vulnerable
3.4.xS	Not vulnerable
3.4.xSG	Not vulnerable
3.5.xS	Not vulnerable
3.5.xE	Not vulnerable
3.6.xS	Not vulnerable
3.6.xE	Not vulnerable
3.7.xS	Not vulnerable
3.8.xS	Not vulnerable
3.9.xS	Not vulnerable
3.10.xS	Not vulnerable
3.11.xS	Vulnerable
3.12.xS	Vulnerable
3.12.0aS	Not vulnerable
3.11.2S	Not vulnerable

Cisco Nexus 1000V Switch for VMware vSphere

The product was initially reported as vulnerable; however, upon additional review it was ascertained that no published releases are vulnerable to this issue.

Workarounds

Cisco has published an Event Response for this vulnerability:
http://www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html

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 updated when information about fixed software versions is available.

Cisco AnyConnect Secure Mobility Client for iOS

Fixed in version 3.0.09353 and available for download on the App Store for devices running iOS version 6 or 7.

Cisco WebEx Meetings Server

Fixed in version 2.0MR2

Cisco TelePresence Video Communication Server (VCS)

Fixed in version X7.2.3 and X8.1.1

Cisco Expressway Series

Fixed in version X8.1.1

Cisco FireAMP Private Cloud Virtual Appliance

Fixed in version 1.0.20140409

After the update:
In order to further secure the Private Cloud instance, it is recommended that customers, after having completed the software update, replace any existing certificates on the appliance:

Customers using certificates other than self-signed certificates should procure and install new certificates. Those certificates should be generated using a new private/public key pair. Customer should NOT reuse the previous public/private keypair. Once replaced, putting the device in and out of maintenance mode will ensure that the new certificates are loaded.

Customers using the default self-signed certificates should generate new certificates after performing the FireAMP Private Cloud update by executing the following commands:

```
amp-ctl maintenance enable
amp-ctl regenerate-ssl-certs
amp-ctl maintenance disable
```

This will regenerate the SSL certificates and restart all of the services.

Additionally, customers should reset all passwords (opadmin and fireamp console) and perform a review of the audit logs in both portals.

Cisco SourceFire

Cisco SourceFire 3D Appliances (running release 4.10.x and 5.x up to 5.3) and Cisco SourceFire SSL appliances are not vulnerable to this issue. These appliances run the 0.9.8 branch of OpenSSL which is not affected by this vulnerability.

For additional information regarding detection, please visit the VRT blog. If you have any questions, please contact Sourcefire Technical Support.

Small Cell Factory Recovery root Filesystem

Fixed software has been deployed to the Cisco USC CloudBase for all FAPs, except the following Products, which are currently in the planning phases of being updated: FPLUS2-000X, G5-000X, G6-000X Series, FEMTOAP-SR1-000X and FEMTOAP-SR2-000X.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is aware that multiple scanning attempts and potentially successful exploitations of the vulnerability described in this advisory are being widely discussed; however, Cisco is not aware of any exploitation of Cisco products or services.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

---

Revision History

Revision 1.26	2014-October-29	Corrected a formatting issue.
Revision 1.25	2014-October-09	Listed the newly released Cisco Unified Communications Domain Manager version 10.1(1) as vulnerable.
Revision 1.24	2014-June-06	Updated the Vulnerable Products and Details sections. Explicitly addressed the Cupid attack.
Revision 1.23	2014-May-23	Updated the Details section. Removed the IOS XE 3.12.0aS version from the vulnerable list as it has been rebuilt to incorporate the fix before the initial release of the target platform.
Revision 1.22	2014-May-22	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, and Details sections. Added the IOS XE 3.12.0aS release to the list of vulnerable ones.
Revision 1.21	2014-May-15	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Upon further investigation the Cisco Edge 300 Digital Media Player was moved to the Products Confirmed Not Vulnerable section.
Revision 1.20	2014-May-09	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. The Cisco Partner Support Services service was moved to the Products Confirmed Not Vulnerable section.
Revision 1.19	2014-May-06	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.18	2014-May-02	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, and Exploitation and Public Announcements sections.
Revision 1.17	2014-April-30	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.16	2014-April-29	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.15	2014-April-28	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, and Details sections.
Revision 1.14	2014-April-25	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, and Software Versions and Fixes.
Revision 1.13	2014-April-24	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, and Details.
Revision 1.12	2014-April-23	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable. The Cisco Nexus 1000V Switch for VMware vSphere was moved to the Products Confirmed Not Vulnerable section.
Revision 1.11	2014-April-22	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, Details and Software Versions and Fixes sections.
Revision 1.10	2014-April-18	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, and Software Versions and Fixes sections.
Revision 1.9	2014-April-17	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.8	2014-April-16	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, Workarounds, and Software Versions and Fixes sections.
Revision 1.7	2014-April-15	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Cisco IP Video Phone E20 marked as not vulnerable. Cisco Prime Security Manager needs further investigation.
Revision 1.6	2014-April-14	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, Workarounds, and Software Versions and Fixes sections. Alphabetized product lists.
Revision 1.5	2014-April-13	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, Details, and Software Versions and Fixes sections.
Revision	2014-April-12	Updated the Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable,

1.4		and Software Versions and Fixes sections.
Revision 1.3	2014-April-11	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.2	2014-April-10	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.1	2014-April-10	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.
Revision 1.0	2014-April-09	Initial public release.

Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

A stand-alone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.