Cisco Security Advisory

SSL Padding Oracle On Downgraded Legacy Encryption (POODLE) Vulnerability

Advisory ID: cisco-sa-20141015-poodle
Last Updated: 2015 November 4 15:40 GMT
Published: 2014 October 15 18:30 GMT
Version1.22: Interim
CVSS Score: Base - 2.6
Workarounds: No workarounds available
Cisco Bug IDs: CSCur23656 CSCur23683 CSCur23698 CSCur23709 CSCur23720 CSCur23727 CSCur26433 CSCur26436 CSCur27131 CSCur27153 CSCur27189 CSCur27340 CSCur27459 CSCur27466 CSCur27477 CSCur27551 CSCur27617 CSCur27691 CSCur27813 CSCur27985 CSCur27999 CSCur28092 CSCur28110 CSCur28114 CSCur28178 CSCur28817 CSCur29000 CSCur29048 CSCur29069 CSCur29078 CSCur29172 CSCur29282 CSCur30345 CSCur30363 CSCur30423 CSCur31566 CSCur31571 CSCur33054 CSCur33203 CSCur33260 CSCur33267 CSCur33274 CSCur33282 CSCur33286 CSCur33289 CSCur33297 CSCur33354 CSCur33929 CSCur34627 CSCur34886 CSCur35067 CSCur36735 CSCur37086 CSCur37317 CSCur38314 CSCur38411 CSCur38418 CSCur38423 CSCur38818 CSCur39303 CSCur39629 CSCur39910 CSCur44194 CSCur45172 CSCur45810 CSCur47726 CSCur49945 CSCur52554 CSCur52967 CSCur54796 CSCus34779 CSCus55522

CVE-2014-3566
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

SSLv3 Cipher Block Chaining Padding Information Disclosure Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

Summary

On October 14, 2014, a vulnerability was publicly announced in the Secure Sockets Layer version 3 (SSLv3) protocol when using a block cipher in Cipher Block Chaining (CBC) mode. SSLv3 is a cryptographic protocol designed to provide communication security, which has been superseded by Transport Layer Security (TLS) protocols. By exploiting this vulnerability, an attacker could decrypt a subset of the encrypted communication.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141015-poodle

Affected Products

Products listed in the Vulnerable Products section of this advisory fit both the following criteria:

- SSLv3 is supported by the product
- A block cipher in CBC mode is one of the transform sets being offered

Products are listed in the Products Confirmed Not Vulnerable section of this advisory if they fit either of the following criteria:

- SSLv3 is not supported by the product
- SSLv3 is supported by the product but no block cipher in CBC mode is offered in the transform set

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.

Products and services listed in the subsections below have had their exposure to this vulnerability confirmed.

Product	Defect	Fixed releases availability
Collaboration and Social Media		
Cisco SocialMiner	CSCur36740	11.0 (Available June 2015)
Cisco WebEx Meetings Server (CWMS)	CSCur23727	2.5MR1 (Available)
Cisco WebEx Node for MCS	CSCuw23863	No further releases planned.
Cisco WebEx Social	CSCur27459	No further releases planned.
Endpoint Clients and Client Software		
Cisco AnyConnect (Android)	CSCur31571	4.0.01110 (Available)
Cisco AnyConnect (Apple iOS)	CSCur31566	3.0.12169 (Available)
Cisco AnyConnect (Win/Mac/Linux)	CSCur27617	Windows: 3.1.05187 (Available) OS X and Linux: 3.1.00495 (Available)
Cisco Jabber Guest	CSCur37086	10.5 (Available)
Cisco Jabber for Android	CSCur33054	10.6 (Available)
Cisco Jabber for Windows	CSCus03203	10.6 (Available)

Network Application, Service, and Acceleration		
Cisco ACE 4710 Application Control Engine (A5)	CSCur27691	A5(3.1b) (Available)
Cisco ACE10 / ACE20 / 4710 (A3x)	CSCur27985	Contact TAC for upgrade options.
Cisco ACE30 Application Control Engine Module	CSCur23683	3.0(0)A5(3.1b) (Available) 3.0(0)A5(3.2) (Available 31-Mar-2015)
Cisco Application and Content Networking System (ACNS)	CSCuu07949	5.5.41 (31-Jul-2015)
Cisco CSS 11500 Series Content Security Switch	CSCur27999	Contact TAC for upgrade options.
Cisco Catalyst 6500 Series Firewall Services Module	CSCur30334	Contact TAC for upgrade options.
Cisco GSS 4492R Global Site Selector	CSCur28817	A patch file is available for affected releases.
Cisco InTracer	CSCur82599	16.0.317 MR (Available)
Cisco Master Content Rating Database Server (MCRDBS)	CSCur86679	15.0 (Available)
Cisco NAC Guest Server	CSCur45172	A patch file is available for affected releases.
Cisco Network Admission Control (NAC)	CSCur30363	A patch file is available for 4.9.4/4.9.3/4.8.3. 4.9.5 (Available)
Cisco Visual Quality Experience Server	CSCur39303	3.9.4 (Available) 3.8.4 (Available) 3.6.9 (Available) 3.7.5 (Available)
Cisco Visual Quality Experience Tools Server	CSCur39303	3.9.4 (Available) 3.8.4 (Available) 3.6.9 (Available) 3.7.5 (Available)
Cisco Wide Area Application Services (WAAS)	CSCur30423	Workaround available - consult bug release note
Network and Content Security Devices		
Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SM)	CSCur30351	Workaround available - consult bug release note.
Cisco Adaptive Security Appliance (ASA)	CSCur23709	9.3.1.1 (Available) 9.2.3(Available) 9.1.5.21 (Available) 9.0.4.26 (Available) 8.4.7.26 (Available) 8.2.5.55 (Available) 8.3.2.43 (Available 30-Apr-2015) 8.5.1.23 (Available 30-Apr-2015) 8.6.1.16 (Available 30-Apr-2015) 8.7.1.15 (Available 30-Apr-2015)
Cisco Content Security Appliance Updater Servers	CSCur70422	Affected systems will be updated by 28-Apr-2015.
Cisco Content Security Management Appliance (SMA)	CSCur27153	9.5 (May 2015)
Cisco Email Security Appliance (ESA)	CSCur27131	9.1 (27-Mar-2015)
Cisco FireSIGHT (Sourcefire Defense Center)	CSCur29974	(A patch file is available for the FireAMP Cloud and Web management UI.) 5.3.0.3 (Available) 5.4.0.1 (Available) 5.3.1.2 (Available) 5.2.0.8 (Available) 4.10.3.11 (Available)
Cisco Identity Service Engine (ISE)	CSCur29078	1.2.0 Patch 13 (Available) 1.2.1 Patch 4 (Available) 1.1.3 Patch 13 (Available) 1.1.4 Patch 13
Cisco Intrusion Prevention System Solutions (IPS)	CSCur29000	7.1(10) (Available 28-May-2015)
Cisco IronPort Encryption Appliance (IEA)	CSCur27340	Workaround available - consult bug release note.
Cisco IronPort Web Security Appliance (WSA)	CSCur27189	9.0.0 (Available Aug 2015) 8.7.0 (Available 30-Mar-2015) 8.8.0 (Available Jun 2015)
Cisco Prime Security Manager (PRSM)	CSCur29172	Workaround available - consult bug release note. 10.6.41 (Available)
Cisco Secure Access Control System (ACS)	CSCur30345	5.5.0.46 (Available) 5.6.0.22 (Available)
Network Management and Provisioning		
Cisco Application Networking Manager	CSCur44194	5.2.5 (Available)
Cisco Intercloud Fabric	CSCur85667	2.2.1 (17-Apr-2015)
Cisco Mobility Unified Reporting System (MUR)	CSCur82552	14.0 (Available)
Cisco NetFlow Generation Appliance (NGA)	CSCur61498	1.0.3 (Available)
Cisco Network Analysis Module	CSCur38314	A patch file is available for affected releases. 6.2 (Available 1-Jun-2015)
Cisco Network Collector	CSCur31455	Workaround available - consult bug release note.
Cisco Packet Tracer	CSCur30224	6.2 (Available)
Cisco Prime Collaboration Deployment	CSCur38423	10.5(2) (Available)
Cisco Prime Collaboration Provisioning	CSCur30586	10.6 (Available)
Cisco Prime Infrastructure Standalone Plug and Play Gateway	CSCus91128	2.2.0.11 (29-May-2015) 3.0 (29-May-2015)
Cisco Prime Infrastructure	CSCur27813	A patch file is available for affected releases.
Cisco Prime LAN Management Solution (LMS - Solaris)	CSCus55522	4.2.5 MR1 (Available) 4.2.5 MR2 (Available) 4.2.5 MR3 (Available June 2015)
Cisco Prime LAN Management Solution (LMS - Windows and Linux)	CSCur38818	4.2.5 MR1 (Available) 4.2.5 MR2 (Available) 4.2.5 MR3 (Available June 2015)
Cisco Prime License Manager	CSCur38418	10.5.2 (Available)
Cisco Prime Network Registrar (CPNR) virtual appliance	CSCur57514	1.9.4 (Available)
Cisco Prime Network Services Controller	CSCur52967	3.4.1b (Available)
Cisco Prime Network	CSCus78642	4.2.2 (31-May-2015)
Cisco Prime Optical	CSCur54796	A patch file is available for the 10.0.2 release. 10.3 (31-Mar-2015)
Cisco Prime Performance Manager	CSCuq35854	1.6 (Available)
Cisco Prime Provisioning	CSCur35067	6.7 (Available)
Cisco Quantum Policy Suite (QPS)	CSCur37107	A patch file is available for affected releases.
Cisco Security Manager	CSCur29069	A patch file is available for affected releases.
Cisco UCS Central	CSCur29282	1.3(1a) (Available 31-Mar-2015)
Cisco Web Element Manager (WEM)	CSCur82499	15.0 (Available)
Local Collector Appliance (LCA)	CSCur30982	2.2.7 (Available)
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 Series	CSCur49945	14.0.25 (Available) 15.0.26 (Available)
Cisco Application Policy Infrastructure Controller (ACI/APIC)	CSCur28110	1.0(2j) (Available) 1.0(1n) (Available)
Cisco IOS and Cisco IOS-XE (IOSd only)	CSCur23656	3.16.0S (31-Jul-2015) 3.15.0S (Available) 3.14.S (Available) 3.12.3 (10-Apr-2015) 3.11.4 (29-May-2015) 3.10.5S (Available) 15.5(3)M (31-Jul-2015) 15.5(2)T (Available) 15.3(3)M5 (Available) 15.1(1)SY5 (Available)
Cisco IOS-XE (CSR1000V management virtual services container)	CSCur97502	3.13.2/15.4(3)S2 (Available) 3.14.1/15.5(1)S1 (Available 13-Mar-2015) 3.15/15.5(2)S (Available 31-Mar-2015)
Cisco IOS-XE (WebUI feature only)	CSCur27466	3.14.1S/15.5(1)S1 (Available) 3.13.2aS/15.4(3)S2a (Available) 3.13.2S/15.4(3)S2 (Available)
Cisco IOS-XR	CSCur26433	5.3.2 (27-Aug-2015)

Cisco Nexus 1000V Series Switches (ESX)	CSCus55315	5.2(1)SV3(1.3) (Available)
Cisco Nexus 1000V Series Switches (Hyper-V)	CSCus15376	5.2(1)SM3(1.2) (15-May-2015)
Cisco Nexus 1000V Series Switches (KVM)	CSCus15345	5.2(1)SK3(2.2) (31-May-2015)
Cisco Nexus 3000 Series Switches	CSCur28178	6.0(2)A4(2) (Available) 6.0(2)U5(1) (Available)
Cisco Nexus 5000	CSCur30094	7.1(1) N1(1) (Available 3-Apr-2015) 7.2(0) N1(1) (Available 8-May-2015)
Cisco Nexus 6000	CSCur30099	7.1(1) N1(1) (Available 3-Apr-2015) 7.2(0) N1(1) (Available 8-May-2015)
Cisco Nexus 7000 and MDS 9000	CSCur26436	Nexus 7000: 6.2(12) (Available) MDS: 5.2(8f) (Available) MDS: 6.2(13) (Available June 2015)
Cisco Nexus 9000 (ACI/Fabric Switch)	CSCur28114	11.0(1d) (Available)
Cisco Nexus 9000 Series (standalone, running NxOS)	CSCur28092	3.2 (Available)
Cisco ONS 15454 Series Multiservice Provisioning Platforms	CSCur45810	10.5.1 (July 2015)
Routing and Switching - Small Business		
Cisco Small Business 200 Series Stackable Managed Switches	CSCut25133	1.4.1.03 (15-May-2015)
Cisco Small Business 300 Series Stackable Managed Switches	CSCut24916	1.4.1.03 (15-May-2015)
Cisco Small Business 500 Series Stackable Managed Switches	CSCut24934	1.4.1.03 (15-May-2015)
Cisco Sx220 switches	CSCut17115	1.4.1 (Available Apr 2015)
Unified Computing		
Cisco Application Virtual Switch (AVS)	CSCus70113	CSCus70113 (Available)
Cisco InterCloud Fabric Virtual Supervisor Module	CSCur88165	2.2.1 (Available 15-Apr-2015)
Cisco Standalone rack server CIMC	CSCur33929	2.0(3f) (Available)
Cisco Unified Computing System (Blade Server)	CSCur29048	3.0.2 (Available) 2.2.4 (Available May 2015)
Cisco Unified Computing System (Management software)	CSCur29264	3.0(2c) (Available) 2.2(3d) (Available) 2.2.4 (Available April 2015)
Cisco Virtual Security Gateway	CSCur95337	5.2(1)VSG2(1.2c) (Available)
Voice and Unified Communications Devices		
Cisco ATA 187 Analog Telephone Adaptor	CSCuu28408	9.2.3.1 ES13 (Available 30-Dec-2015)
Cisco Computer Telephony Integration Object Server (CTIOS)	CSCur46589	11.0(1) (Available) 9.04 (Available 31-Mar-2015) 10.0(2) (Available 30-Apr-2015) 10.5(2) (Available 30-Apr-2015)
Cisco DX Series IP Phones	CSCur37317	10.2.3(26) (Available) 10.2.3(33) (Available)
Cisco Emergency Responder	CSCur38406	10.5.1.10000-5 (Available)
Cisco Finesse	CSCur36742	10.6.1 (Available) 11.0.1 (Available 30-Apr-2015)
Cisco IM and Presence Service (Cisco UPS)	CSCur33203	8.6.5 SU5 (15-Jul-2015) 9.1.1 SU5 (10-Apr-2015)
Cisco IP Phone 8800 Series	CSCus33504	10.3.1 (31-Mar-2015)
Cisco Jabber for Apple iOS	CSCur88532	10.6 (Available)
Cisco MediaSense	CSCur36737	11.0 (30-May-2015)
Cisco Paging Server	CSCur73771	9.1.1 (Available)
Cisco Real Time Monitoring Tool	CSCus76752	9.1(2)SU3 (Available)
Cisco SPA112 2-Port Phone Adapter	CSCur30751	1.3.6 (Available 11-Nov-2015)
Cisco SPA122 ATA with Router	CSCur30751	1.3.6 (Available 11-Nov-2015)
Cisco SPA232D Multi-Line DECT ATA	CSCur30751	1.3.6 (Available 11-Nov-2015)
Cisco SPA525G	CSCur30683	7.5.7 (Available)
Cisco Unified 6900 series IP Phones	CSCus72472	9.4.(1)SR2 - SCCP (Available June 2015) 9.4(1)SR1 - SIP (Available June 2015)
Cisco Unified 6945 IP Phones	CSCus33517	9.4(1)ES10 (Available)
Cisco Unified 7800 series IP Phones	CSCus33522	10.3.1 (30-Apr-2015)
Cisco Unified 8945 IP Phone	CSCus33509	9.4(2)SR1 (Available)
Cisco Unified 8961 IP Phone	CSCus33551	9.4(2)SR1 (Available)
Cisco Unified 9951 IP Phone	CSCus33551	9.4(2)SR1 (Available)
Cisco Unified 9971 IP Phone	CSCus33551	9.4(2)SR1 (Available)
Cisco Unified Communications Domain Manager v10	CSCus31279	10.1.2 (Available)
Cisco Unified Communications Domain Manager v8	CSCur31551	A patch file is available for releases 8.1.4 and prior. 8.1.5 (Available 30-Jun-2015) 8.1.6 (December 2015)
Cisco Unified Communications Manager (Cisco UCM)	CSCur23720	10.5.2SU2 (31-May-2015)
Cisco Unified Communications for Microsoft Lync	CSCus17232	10.6 (Available)
Cisco Unified Contact Center Enterprise (UCCE)	CSCur46573	11.0(1) (Available) 9.04 (Available 31-Mar-2015) 10.0(2) (Available 30-Apr-2015) 10.5(2) (Available 30-Apr-2015)
Cisco Unified Contact Center Express (UCCX)	CSCur36735	10.6(1) (Available)
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	CSCus73694	9.3(5) (Available 31-Aug-2015)
Cisco Unified IP Phone 7900 Series	CSCus33571	9.4(2)SR1 (Available mid-April 2015)
Cisco Unified Intelligence Center (CUIC)	CSCur36747	11.0(1) (June 2015)
Cisco Unified MeetingPlace	CSCur33354	A patch file is available for affected releases.
Cisco Unified Operations Manager (CUOM)	CSCus61254	Contact TAC for upgrade options.
Cisco Unified Wireless IP Phone	CSCus34779	1.4.7 (Available 1-Jun-2015)
Cisco Unified Workforce Optimization Quality Management	CSCur86091	10.5(1)SR5 (Available)
Cisco Unity Connection (UC)	CSCur38411	9.1.2SU3 (Available) 10.5.2 (Available)
Cisco Voice Portal (CVP)	CSCus00447	11.0(1) (June 2015)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco DCM Series 990x-Digital Content Manager	CSCur34886	1.5.10 (Available)
Cisco Edge 300 Digital Media Player	CSCur52554	1.6RB(2) (13-Mar-2015)
Cisco Edge 340 Digital Media Player	CSCur47726	1.2 (Available) 1.1.0.4 (Available)
Cisco Explorer Controller	CSCut06313	8.0 (15-Jan-2016)
Cisco Expressway Series	CSCur35544	X8.5 RC2 (Available)
Cisco Media Experience Engines (MXE)	CSCus77133	A patch file is available for affected releases.
Cisco TelePresence Advanced Media Gateway 3610	CSCur33286	1.1(1.40) (Available)
Cisco TelePresence Conductor	CSCur36046	XC3.0 (Available)
Cisco TelePresence EX Series	CSCur23723	7.3 (Available)
Cisco TelePresence IP Gateway Series	CSCur33289	Contact TAC for upgrade options.
Cisco TelePresence IP VCR Series	CSCur33294	Contact TAC for upgrade options.
Cisco TelePresence ISDN Gateway	CSCur33282	2.2 Maintenance Release 4 (Available 30-Apr-2015)
Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)	CSCur33260	4.5(1.55) (Available)
Cisco TelePresence MPS Series	CSCur33284	Contact TAC for upgrade options.
Cisco TelePresence MSE 8050 Supervisor	CSCur33267	2.3 (Available)
Cisco TelePresence MX Series	CSCur23723	7.3 (Available)
Cisco TelePresence Manager (CTSMan)	CSCur53414	1.9.4 (Available)
Cisco TelePresence Multipoint Switch (CTMS)	CSCus21874	Contact TAC for upgrade options.
Cisco TelePresence Profile Series	CSCur23723	7.3 (Available)
Cisco TelePresence SX Series	CSCur23723	7.3 (Available)
Cisco TelePresence Serial Gateway Series	CSCur33297	1.0(1.42) (Available)

Cisco TelePresence Server 8710 and 7010	CSCur33274	4.1 (Available)
Cisco TelePresence Server 8710, 7010	CSCur29295	4.1(1.79) (Available)
Cisco TelePresence Server on Multiparty Media 310, 320	CSCur29295	4.1(1.79) (Available)
Cisco TelePresence Server on Multiparty Media 310, 320	CSCur33274	4.1 (Available)
Cisco TelePresence Server on Virtual Machine	CSCur29295	4.1(1.79) (Available)
Cisco TelePresence Server on Virtual Machine	CSCur33274	4.1 (Available)
Cisco TelePresence System 3000 Series	CSCut20638	1.10.11 (Available 30-Apr-2015) 6.1.8 (Available 30-Apr-2015)
Cisco TelePresence Video Communication Server (VCS)	CSCur35544	X8.5 RC2 (Available)
Cisco Telepresence Integrator C Series	CSCur23723	7.3 (Available)
Cisco Video Distribution Suite	CSCur39629	3.3.1 (Available) 4.0.0 (Available)
Cisco Videoscape Control Suite Foundation	CSCur52786	4.0.2 (Available 15-Jan-2016)
Cisco Videoscape Distribution Suite for Internet Streaming	CSCur47193	3.3.1-b113 (Available)
Wireless		
Cisco Mobility Service Engine (MSE)	CSCur45764	8.0 MR1 (Available)
Cisco Wireless Control System (WCS)	CSCur69679	Contact TAC for upgrade options.
Cisco Wireless LAN Controller (WLC)	CSCur27551	8.0.110.0 (Available) 7.0.251.0 (Available) 7.4.130.0 (Available)
Cisco Wireless Location Appliance (WLA)	CSCur45764	8.0 MR1 (Available)
Cisco Hosted Services		
Cisco Cloud Web Security (CWS)	CSCur34051	Resolved in CWS components (Portal/Hosted Config/HTTPS Inspect)
Cisco Common Services Platform Collector	CSCur27898	2.3.8 (Available) 2.4.2 (Available) 3.0.0.1 (Available)
Cisco Proactive Network Operations Center	CSCur39184	Affected systems have been patched.
Cisco Registered Envelope Service (CRES)	CSCur27657	Affected systems have been patched.
Cisco Services Provisioning Platform (SPP)	CSCur30533	Affected servers have been patched.
Cisco UCS Invicta Series Autosupport Portal	CSCur29802	Affected systems have been patched.
Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center)	CSCur45445	T29SP11 (Available December 2015) T28.12EP27 (Available December 2015)
Cisco Webex Messenger Service	CSCur31504	Affected systems will be patched by 2-Apr-2015
Network Change and Configuration Management	CSCur31043	2.6 (Available)

Products Confirmed Not Vulnerable

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

Endpoint Clients and Client Software

- Cisco IP Communicator

Network and Content Security Devices

- Cisco Adaptive Security Device Manager (ASDM)
- Cisco PIX

Network Management and Provisioning

- Cisco Access Registrar Appliance
- Cisco MGC Node Manager
- Cisco Prime Access Registrar Appliance
- Cisco Prime Data Center Network Manager
- CiscoWorks Network Compliance Manager

Voice and Unified Communications Devices

- Cisco 7937 IP Phone
- Cisco Billing and Measurements Server (BAMS)
- Cisco PSTN Gateway (PGW) 2200
- Cisco TAPI Service Provider (TSP)
- Cisco Unified 8831 series IP Conference Phone
- Cisco Unified IP Phone 6901 and 6911
- Cisco Unified Sip Proxy

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco D9824 Advanced Multi Decryption Receiver
- Cisco D9854/D9854-I Advanced Program Receiver
- Cisco D9858 Advanced Receiver Transcoder
- Cisco D9859 Advanced Receiver Transcoder
- Cisco TelePresence Management Suite

Cisco Hosted Services

- Connected Analytics for Network Deployment (CAND)
- Services Analytic Platform

Details

SSLv3 is a cryptographic protocol used to provide security for communications over Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) data networks, such as the Internet. A vulnerability was publicly announced in the SSLv3 protocol when using a block cipher in CBC mode. The vulnerability exists because the block cipher padding is not covered by the message authentication code and exposes users to a potential man-in-the-middle attack that relies on padding oracles. Because weaknesses have previously been discovered in stream ciphers such as RC4 in the SSLv3 protocol, the whole protocol should now be considered deprecated. This vulnerability is related to the protocol itself and is not specific to a particular SSLv3 implementation.

Current clients negotiate TLS by default, but they can fall back to SSLv3 if the negotiation to use TLS has failed. An attacker performing a man-in-the-middle attack could trigger a protocol downgrade to SSLv3 and exploit this vulnerability to decrypt a subset of the encrypted communication.

SSLv3 is used by various features in Cisco products, for example, web-based administration interfaces over HTTPS, SSL VPNs, Secure SIP, or file transfer over HTTPS.

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2014-3566.

Workarounds

There are no workarounds for customers requiring the functionality provided by the SSLv3 protocol.

Customers not requiring the SSLv3 protocol to be enabled may proactively disable it to prevent exploitation of this vulnerability. Please consult your Cisco product documentation for instructions on how to disable the SSLv3 protocol on your specific Cisco product.

Note: Disabling the SSLv3 protocol may impact connectivity or interoperability with some clients and servers.

Cisco has published an Event Response for this vulnerability:
http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html

Fixed Software

Please consult the release notes of the respective bugs to find information about software versions and fixes.

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.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of the vulnerability that is described in this advisory.

This vulnerability was reported to Cisco by Bodo Moeller from Google.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141015-poodle

---

Revision History

Version	Description	Section	Status	Date
1.22	Modified the ETA for the fix for Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center).	Vulnerable Products	Interim	2015-November-04
1.21	Added Cisco WebEx Node for MCS to the Vulnerable Products section and Cisco TAPI Service Provider (TSP) and Cisco IP Communicator to the Products Confirmed Not Vulnerable section.	Vulnerable Products and Products Confirmed Not Vulnerable	Interim	2015-October-22
1.20	Metadata update. No changes to the advisory.			2015-July-09
1.20	Added Cisco ATA 187 Analog Telephone Adaptor to the Vulnerable Products section and Cisco TelePresence Management Suite (TMS) to the Products Not Vulnerable section. Updated fixed release information for several products.			2015-June-25
1.19	Added Cisco Application and Content Networking System (ACNS) to the Vulnerable Products section. Updated fixed release information for several products.			2015-May-07
1.18	Added Cisco Intercloud Fabric, Cisco InterCloud Fabric Virtual Supervisor Module, Cisco Real Time Monitoring Tool, Cisco Explorer Controller, Cisco TelePresence System 3000 Series, Cisco Sx300 switches, Cisco Sx500 switches, and Cisco Sx200 switches to the Vulnerable Products section. Updated fixed releases information for several products.			2015-April-09
1.17	Moved Cisco Access Registrar Appliance and Cisco Prime Access Registrar Appliance to Not Vulnerable section from Vulnerable section. Moved Cisco Packet Tracer, Cisco MediaSense, and Cisco WebEx Messenger Service to Vulnerable section from Not Vulnerable section. Added Cisco Unified 8831 Series IP Conference Phone Enterprise to Not Vulnerable section. Updated fixed releases information for several products.			2015-March-24
1.16	Table version for the Vulnerable products section. More products added.			2015-March-12
1.15	Added Cisco Prime Performance Manager, Cisco Application Virtual Switch (AVS), Cisco Unified 7800 series IP Phones to the Vulnerable Products section. Changed category of Cisco UCS Invicta Series Autosupport Portal. Added CiscoWorks Network Compliance Manager to the Not Vulnerable products section.			2015-February-27
1.14	Added Cisco Prime LAN Management Solution (LMS - Solaris), Cisco Prime Network, Cisco Unified 6900 series IP Phones, Cisco Unified IP Conference Phone 8831, Cisco Unified Wireless IP Phone to the Vulnerable Products section.			2015-February-23
1.13	Moved or added Cisco IOS-XE (CSR1000V management virtual services container), Cisco Virtual Security Gateway, Cisco IP Phone 8800 Series, Cisco SPA525G, Cisco Unified 8961 IP Phone, Cisco Unified 9951 IP Phone, Cisco Unified 9971 IP Phone, Cisco Unified IP Phone 7900 Series, Cisco Unified Operations Manager (CUOM), Cisco Unified Workforce Optimization Quality Management, Cisco TelePresence Multipoint Switch (CTMS), Cisco Unified Communications Domain Manager v8, Cisco Unified Communications Domain Manager v10, Cisco Unified Wireless IP Phone to the Vulnerable Products section. Updated Products Not Vulnerable section. Removed Products Under Investigation section.			2015-January-29
1.12	Moved Cisco Catalyst 6500 Series Firewall Services Module, Cisco InTracer, Cisco Master Content Rating Database Server (MCRDBS), Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SM), Cisco Content Security Appliance Updater Servers, Cisco Mobility Unified Reporting System (MUR), Cisco Quantum Policy Suite (QPS), Cisco Web Element Manager (WEM), Cisco SPA112 2-Port Phone Adapter, Cisco SPA122 ATA with Router, Cisco SPA232D Multi-Line DECT ATA, Cisco Voice Portal (CVP), Cisco TelePresence Manager (CTSMan), Cisco Videoscape Control Suite Foundation, Cisco Mobility Service Engine (MSE), Cisco Wireless Control System (WCS), Cisco Wireless Location Appliance (WLA), Cisco Services Provisioning Platform (SPP) to the Vulnerable Products section. Updated Products Not Vulnerable and Products Under Investigation sections.			2014-December-12
1.11	Moved Cisco Network Collector, Cisco Prime Collaboration Provisioning, Cisco Unified Intelligence Center (UIC), Cisco Computer Telephony Integration Object Server (CTIOS), Cisco Emergency Responder, Cisco Paging Server, Cisco Unified Contact Center Enterprise (UCCE), Cisco Videoscape Distribution Suite for Internet Streaming to the Vulnerable Products section. Updated Products Not Vulnerable and Products Under Investigation sections.			2014-November-21
1.10	Moved Cisco NetFlow Generation Appliance (NGA), Cisco Finesse, Cisco SocialMiner, Cisco Expressway Series, Cisco TelePresence Conductor, Cisco TelePresence Video Communication Server (VCS), and Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, and Support Center) to the Vulnerable Products section. Updated Products Not Vulnerable and Products Under Investigation sections.			2014-November-13
1.9	Moved Cisco WebEx Meetings Server (CWMS), Cisco GSS 4492R Global Site Selector, Cisco Wide Area Application Services (WAAS), Cisco FireSIGHT (Sourcefire Defense Center), Cisco Application Networking Manager, Cisco Prime Network Services Controller, Cisco Prime Optical, Cisco UCS Central, Local Collector Appliance (LCA), Cisco ASR 5000 Series, Cisco IOS-XE (WebUI feature), Cisco Nexus 5000, Cisco Nexus 6000, Cisco Unified MeetingPlace, Cisco Unity Connection (UC), Cisco Edge 300 Digital Media Player, Cisco TelePresence EX Series, Cisco TelePresence MX Series, Cisco TelePresence Profile Series, Cisco TelePresence SX Series, Cisco Telepresence Integrator C Series, and Network Change and Configuration Management to Vulnerable Products section. Updated Products Not Vulnerable and Products Under Investigation sections.			2014-November-07
1.8	Moved Cisco Jabber for Android, Cisco Content Security Management Appliance (SMA), Cisco Registered Envelope Service (CRES), Cisco Prime Collaboration Deployment, Cisco Prime License Manager, Cisco Security Manager, Cisco Nexus 7000 and MDS 9000, and Cisco Proactive Network Operations Center to Vulnerable Products section. Updated Products Not Vulnerable and Products Under Investigation sections.			2014-October-31
1.7	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.			2014-October-29
1.6	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.			2014-October-28
1.5	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.			2014-October-24
1.4	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.			2014-October-20
1.3	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.			2014-October-17
1.2	Added Products to the Vulnerable Products section.			2014-October-16
1.1	Added Event Response link.			2014-October-15
1.0	Initial public release.			2014-October-15

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 standalone 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.