SSL Padding Oracle On Downgraded Legacy Encryption (POODLE) Vulnerability

Advisory ID：cisco-sa-20141015-poodle

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

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

Revision 1.20

Last Updated 2015 June 25 16:26 UTC (GMT)

For Public Release 2014 October 15 18:30 UTC (GMT)

目次

要約

Cypher Block Chaining (CBC) モードでブロック暗号を使用した場合、セキュア ソケット レイヤ バージョン 3 (SSLv3) プロトコルに脆弱性が存在することが、2014 年 10 月 14 日に発表されました。SSLv3 は通信セキュリティを提供するために設計された暗号化プロトコルで、すでに Transport Layer Security (TLS) プロトコルへの置き換えが進んでいます。この脆弱性の不正利用に成功した場合、攻撃者は暗号化された通信のサブセットを復号化できる可能性があります。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141015-poodle

該当製品

次の両方の条件を満たす製品が、このセキュリティ アドバイザリの「脆弱性が認められる製品」

セクションに記載されています。

- SSLv3 をサポートしている
- トランスフォーム セットの 1 つとして CBC モードでのブロック暗号を提供している

次の条件のいずれかを満たす製品が、このセキュリティ アドバイザリの「脆弱性が認められない製品」セクションに記載されています。

- SSLv3 をサポートしていない
- SSLv3 をサポートしているが、トランスフォーム セットの 1 つとして CBC モードでのブロック暗号を提供していない

脆弱性が認められる製品

以下のバグの進捗をを確認するには、 Cisco Bug Search Tool で詳細をご確認ください。 *Save Bug* を選択し、 *Email Notification* 機能を用いてバグに更新があった際に自動で通知を受け取ることもできます。

このサブセクションに記載されている製品とサービスは、この脆弱性の影響を受けることが確認されています。

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 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	
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	CSCut25133	1.4.1.03 (15-May-2015)

Switches		
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	CSCur52554	1.6RB(2) (13-Mar-2015)

Media Player		
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 September 2015) T28.12EP27 (Available September 2015)
Cisco Webex Messenger Service	CSCur31504	Affected systems will be patched by 2-Apr-2015
Network Change and Configuration Management	CSCur31043	2.6 (Available)

脆弱性が認められない製品

分析の結果、次のシスコ製品はこれらの脆弱性の影響を受けないことがわかっています。

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 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

詳細

SSLv3 は、インターネット プロトコル バージョン 4（IPv4）およびインターネット プロトコル バージョン 6（IPv6）データ ネットワーク上でのインターネット通信などにおいてセキュリティを提供するために使用される暗号化プロトコルです。CBC モードでブロック暗号を使用する場合、SSLv3 プロトコルに脆弱性が存在することが発表されました。ブロック暗号パディングがメッセージ認証コードの対象となっておらず、パディング オラクルを使用した中間者攻撃を受ける可能性があります。SSLv3 プロトコルではこれまでに、RC4 などのストリーム暗号で弱点があることが発見されており、このプロトコルの使用を廃止することが推奨されます。この脆弱性はプロトコルそのものに関連するものであり、特定の SSLv3 の実装に限定されるものではありません。

現在のクライアントはデフォルトで TLS ネゴシエーションを行いますが、TLS を使用したネゴシエーションが失敗すると SSLv3 にフォールバックされる可能性があります。中間者攻撃を実行する攻撃者によって、プロトコルの SSLv3 へのダウングレードがトリガーされる可能性があり、この脆弱性を利用することで、暗号化された通信のサブセットが復号化される可能性があります。

SSLv3 は、HTTPS、SSL VPN、Secure SIP を使用した Web ベースの管理インターフェイスや

、HTTPS でのファイル転送など、シスコ製品のさまざまな機能で使用されています。

Common Vulnerabilities and Exposures（CVE）ID として CVE-2014-3566 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

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

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

シスコは次のリンクで CVSS に関する追加情報を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

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

SSL Padding Oracle On Downgraded Legacy Encryption (POODLE) Vulnerability					
CVSS Base Score - **2.6**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Partial	None	None
CVSS Temporal Score - **2.5**					
Exploitability		Remediation Level		Report Confidence	
Functional		Unavailable		Confirmed	

影響

この脆弱性が不正利用されると、暗号化された通信のサブセットが攻撃者によって復号化される可能性があります。

ソフトウェア バージョンおよび修正

ソフトウェア バージョンと修正についての情報は、それぞれのバグのリリース ノートをご参照ください。

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

回避策

SSLv3 プロトコルによって提供される機能を必要とするユーザには、回避策はありません。

SSLv3 プロトコルを有効にしておく必要がないユーザは、この脆弱性の不正利用を防ぐため、あらかじめ無効にしておくことが可能です。特定のシスコ製品で SSLv3 プロトコルを無効にする方法については、ご利用のシスコ製品のマニュアルをご確認ください。

注：SSLv3 プロトコルを無効にすると、一部のクライアントおよびサーバとの接続や相互運用性に影響が生じる場合があります。

シスコはこの脆弱性についてイベント レスポンスを公開しています。
http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html

修正済みソフトウェアの入手

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

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

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

サードパーティのサポート会社をご利用のお客様

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

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適で

あることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

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

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

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

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のいかなる不正利用事例も確認しておりません。

この脆弱性は、Google の Bodo Moeller 氏によってシスコに報告されました。

この通知のステータス：Interim

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証を示唆するものでもありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

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

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141015-poodle

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

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

- cisco-nsp@puck.nether.net
- fulldisclosure@seclists.org

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

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

更新履歴

Revision 1.20	2015-June-25	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.
Revision 1.19	2015-May-07	Added Cisco Application and Content Networking System (ACNS) to the Vulnerable Products section. Updated fixed release information for several products.
Revision 1.18	2015-April-09	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.
Revision 1.17	2015-March-24	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.
Revision 1.16	2015-March-12	Table version for the Vulnerable products section. More products added.
Re	2015-	Added Cisco Prime Performance

visi on 1.1 5	February -27	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.
Re visi on 1.1 4	2015- February -23	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.
Re visi on 1.1 3	2015- January- 29	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.
Re visi on 1.1 2	2014- Decembe r-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.
Revision 1.11	2014-November-21	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.
Revision 1.10	2014-November-13	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.
Revision 1.9	2014-November-07	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.
Revision 1.8	2014-October-31	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, Products Under Investigation sections.
Revision 1.7	2014-October-29	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.
Revision 1.6	2014-October-28	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.
Revision 1.5	2014-October-24	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.
Revision 1.4	2014-October-20	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.
Revision 1.3	2014-October-17	Updated Vulnerable Products, Products Not Vulnerable, Products Under Investigation sections.
Revision 1.2	2014-October-16	Added Products to the Vulnerable Products section.
Revision 1.1	2014-October-15	Added Event Reponse link.
Revision 1.0	2014-October-15	Initial public release.

シスコ セキュリティ手順

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