

# シスコ製品に影響するOpenSSLの複数の脆弱性 : 2016年3月



アドバイザーID : [cisco-sa-20160302-openssl](#) [CVE-2016-0800](#)  
初公開日 : 2016-03-02 12:30 [CVE-2016-0799](#)  
最終更新日 : 2016-05-23 14:04 [CVE-2016-0798](#)  
バージョン 2.2 : Interim [CVE-2016-0798](#)  
回避策 : No workarounds available [CVE-2016-0797](#)  
Cisco バグ ID : [CSCuy54659](#) [CSCuy54539](#) [CVE-2016-0797](#)  
[CSCuy54536](#) [CSCuy54657](#) [CSCuy54537](#) [CVE-2016-2842](#)  
[CSCuy54534](#) [CSCuy54655](#) [CSCuy54535](#) [CVE-2016-2842](#)  
[CSCuy54665](#) [CSCuy54541](#) [CSCuy54662](#) [CVE-2016-0705](#)  
[CSCuy54542](#) [CSCuy54660](#) [CSCuy54540](#) [CVE-2016-0705](#)  
[CSCuy54549](#) [CSCuy54547](#) [CSCuy54668](#) [CVE-2016-0704](#)  
[CSCuy54545](#) [CSCuy54546](#) [CSCuy54433](#) [CVE-2016-0704](#)  
[CSCuy54676](#) [CSCuy54674](#) [CSCuy54551](#) [CVE-2016-0703](#)  
[CSCuy54672](#) [CSCuy62564](#) [CSCuy54558](#) [CVE-2016-0703](#)  
[CSCuy54679](#) [CSCuy54436](#) [CSCuy54687](#) [CVE-2016-0702](#)  
[CSCuy54564](#) [CSCuy74294](#) [CSCuy74297](#) [CVE-2016-0702](#)  
[CSCuy54560](#) [CSCuy74298](#) [CSCuy58091](#)  
[CSCuy58090](#) [CSCuy54569](#) [CSCuy54567](#)  
[CSCuy54600](#) [CSCuy54688](#) [CSCuy54601](#)  
[CSCuy54455](#) [CSCuy54576](#) [CSCuy54577](#)  
[CSCuy54453](#) [CSCuy54575](#) [CSCuy54696](#)  
[CSCuy54451](#) [CSCuy54452](#) [CSCuy58096](#)  
[CSCuy58094](#) [CSCuy54616](#) [CSCuy54457](#)  
[CSCuy54611](#) [CSCuy54458](#) [CSCuy54579](#)  
[CSCuy54612](#) [CSCuy54587](#) [CSCuy54500](#)  
[CSCuy54585](#) [CSCuy54465](#) [CSCuy54586](#)  
[CSCuy54463](#) [CSCuy54584](#) [CSCuy54460](#)  
[CSCuy54580](#) [CSCuy54628](#) [CSCuy54508](#)  
[CSCuy54505](#) [CSCuy54626](#) [CSCuy54506](#)  
[CSCuy53654](#) [CSCuy54504](#) [CSCuy54502](#)  
[CSCuy54623](#) [CSCuy54510](#) [CSCuy54631](#)  
[CSCuy54478](#) [CSCuy54599](#) [CSCuy54630](#)  
[CSCuy54473](#) [CSCuy54474](#) [CSCuy54595](#)  
[CSCuy54472](#) [CSCuy54518](#) [CSCuy54639](#)  
[CSCuy54516](#) [CSCuy54637](#) [CSCuy54517](#)  
[CSCuy54514](#) [CSCuy54636](#) [CSCuy53668](#)

[CSCuy54479](#) [CSCuy54512](#) [CSCuy54513](#)  
[CSCuy54488](#) [CSCuy54521](#) [CSCuy54522](#)  
[CSCuy54640](#) [CSCuy54520](#) [CSCuy54485](#)  
[CSCuy54529](#) [CSCuy54527](#) [CSCuy54525](#)  
[CSCuy54646](#) [CSCuy58728](#) [CSCuy58727](#)  
[CSCuy54524](#) [CSCuy54645](#) [CSCuy54499](#)  
[CSCuy54532](#) [CSCuy54533](#) [CSCuy54654](#)  
[CSCuy54652](#) [CSCuy59818](#) [CSCuy54492](#)

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。

## 概要

2016年3月1日、OpenSSL Software Foundationは、7つの脆弱性を詳述したセキュリティアドバイザリと、廃止および弱体化した暗号化(DROWN)によるRSAの復号化攻撃と呼ばれる新しい攻撃をリリースしました。合計8つのCommon Vulnerabilities and Exposures(CVE)が割り当てられました。8つのCVEのうち、3つはDROWN攻撃に関連しています。残りのCVEは、重大度の低い脆弱性を追跡します。

DROWNは、SSLバージョン2(SSLv2)の脆弱性をアクティブに不正利用して、パッシブに収集されたTransport Layer Security(TLS)セッションを復号化するクロスプロトコル攻撃です。DROWNは、TLSプロトコルの脆弱性やプロトコルの特定の実装を不正利用しません。

DROWN攻撃を成功させるには、攻撃者はSSLv2とTLSの両方をサポートし、両方のプロトコルに同じRSAキーペアを使用するサーバを特定する必要があります。攻撃者は、サーバのTLSトラフィックを収集できる必要もあります。

このアドバイザリは追加情報が入手可能になった時点で更新されます。

このアドバイザリは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl>

## 該当製品

シスコでは現在、本脆弱性の影響を受ける製品と影響の範囲を特定するために、製品ラインを調査中です。このドキュメントでは、調査の進展に応じて、影響を受ける製品の Cisco Bug ID が更新されます。Cisco Bug ID は [Cisco Bug Search Tool](#) を使用してアクセス可能であり、[回避策 \(使用可能な場合\)](#) と修正されたソフトウェアバージョンなど、プラットフォーム固有の追加情報が含まれます。

以下の製品については、本アドバイザリに記載された脆弱性の影響に関して現在調査中です。

## 調査中の製品

### Unified Computing

- Cisco UCS Invicta Series Solid State Systems

### シスコ ホステッド サービス

- Cisco UCS Invicta Series Autosupport Portal

## 脆弱性のある製品

次の表に、本アドバイザリに記載された1つ以上の脆弱性の影響を受けるシスコ製品を示します。

重要：次の表では、製品名の後にあるアスタリスク(\*)は、DROWN攻撃に対して脆弱なシスコ製品を示しています。このドキュメントの発行時点で、25のシスコ製品がDROWN攻撃に対して脆弱であることが確認されています。

製品	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco MeetingPlace	<a href="#">0.CSCuy54660</a>	
Cisco SocialMiner	<a href="#">0.CSCuy74298</a>	
Cisco WebEx Meetings Server versions 1.x	<a href="#">0.CSCuy54463</a>	2.6.2 ( 2016年4月15日 )
Cisco WebEx Meetings Server versions 2.x	<a href="#">0.CSCuy54463</a>	2.6.2 ( 2016年4月15日 )
Cisco WebEx Node for MCS	<a href="#">0.CSCuy54457</a>	
エンドポイント クライアントとクライアント ソフトウェア		
Cisco Agent for OpenFlow	<a href="#">0.CSCuy54595</a>	
Cisco AnyConnect Secure Mobility Client for Android	<a href="#">0.CSCuy54599</a>	
Cisco AnyConnect Secure Mobility Client for Android	<a href="#">0.CSCuy54600</a>	
Cisco AnyConnect Secure Mobility Client for Linux	<a href="#">0.CSCuy54599</a>	
Cisco AnyConnect Secure Mobility	<a href="#">0.CSCuy54599</a>	

Client for OS X		
Cisco AnyConnect Secure Mobility Client for Windows	<a href="#">0.CSCuy54599</a>	
Cisco AnyConnect Secure Mobility Client for iOS	<a href="#">0.CSCuy54599</a>	
Cisco Jabber Guest 10.0(2)	<a href="#">0.CSCuy54659</a>	
Cisco Jabber Software Development Kit	<a href="#">0.CSCuy54657</a>	
Cisco Jabber for Android	<a href="#">0.CSCuy54676</a>	
Cisco Jabber for Mac	<a href="#">0.CSCuy59818</a>	11.6 ( 2016年3月23日 ) 11.7 ( 2016年3月23日 )
Cisco Jabber for Windows	<a href="#">0.CSCuy62564</a>	
Cisco MMP サーバ	<a href="#">0.CSCuy54470</a>	
Cisco Webex Meetings Client - ホスト型	<a href="#">0.CSCuy54468</a>	
Cisco WebEx Meetingsクライアント - オンプレミス	<a href="#">0.CSCuy54461</a>	
Cisco WebEx Meetings for Android	<a href="#">0.CSCuy54458</a>	
Cisco WebEx Meetings for WP8	<a href="#">0.CSCuy54460</a>	
JCF コンポーネント	<a href="#">0.CSCuy56053</a>	11.6 ( 2016年3月23日 )
WebEx Meetings Server - SSL Gateway	<a href="#">0.CSCuy54464</a>	2.6.2 ( 2016年4月15日 )
WebEx Recording Playback Client	<a href="#">0.CSCuy54467</a>	
ネットワーク アプリケーション、サービス、およびアクセラレーション		
Cisco ACE 30 Application Control Engine Module	<a href="#">0.CSCuy54474</a>	
Cisco ACE 4710 Application Control Engine ( A5 )	<a href="#">0.CSCuy54474</a>	
Cisco Application and Content Networking System(ACNS)(*)	<a href="#">0.CSCuy54560</a>	5.5.41 ( 2016年4月15日 )
Cisco InTracer	<a href="#">0.CSCuy54435</a>	
Cisco Network Admission Control (NAC)	<a href="#">0.CSCuy54561</a>	
Cisco Visual Quality Experience Server	<a href="#">0.CSCuy54558</a>	
Cisco Visual Quality Experience	<a href="#">0.CSCuy54558</a>	

Tools Server		
Cisco Wide Area Application Services ( WAAS )	<a href="#">0.CSCuy58094</a>	
ネットワークおよびコンテンツ セキュリティ デバイス		
Cisco ASA CX と Cisco Prime Security Manager	<a href="#">0.CSCuy54575</a>	9.3.4.5 ( 2016年5月30日 )
Cisco ASA Next-Generation Firewall Services	<a href="#">0.CSCuy54572</a>	
Cisco Adaptive Security Appliance ( ASA )	<a href="#">0.CSCuy54567</a>	
Cisco Clean Access Manager	<a href="#">0.CSCuy54562</a>	
Cisco Content Security Appliance Updater Servers	<a href="#">0.CSCuy54455</a>	
Cisco Content Security Management Appliance (SMA)	<a href="#">0.CSCuy53668</a>	
Cisco Email Security Appliance (ESA)	<a href="#">0.CSCuy53654</a>	10.0 ( 2016年6月下旬 )
Cisco FireSIGHT システム ソフトウェア	<a href="#">0.CSCuy54453</a>	
Cisco IPS(*)	<a href="#">0.CSCuy54601</a>	7.1(11)パッチ2 ( 2016年8月 ) 7.3(05)パッチ2 ( 2016年11月 )
Cisco Identity Services Engine ( ISE )	<a href="#">0.CSCuy54586</a>	
Cisco IronPort Encryption Appliance ( IEA )	<a href="#">0.CSCuy54452</a>	製品がEoLであるため、修正は予定されていません。
Cisco NAC Guest Server	<a href="#">0.CSCuy54564</a>	
Cisco NAC Server	<a href="#">0.CSCuy54563</a>	
Cisco Physical Access Control Gateway	<a href="#">0.CSCuy54579</a>	
Cisco Secure Access Control Server ( ACS )	<a href="#">0.CSCuy54597</a>	
Cisco Virtual Security Gateway for Microsoft Hyper-V	<a href="#">0.CSCuy54498</a>	
Cisco Web Security Appliance (WSA)	<a href="#">0.CSCuy54456</a>	10.0 ( 2016年6月下旬 )
ネットワーク管理とプロビジョニング		
Cisco Application Networking	<a href="#">0.CSCuy54475</a>	

Manager		
Cisco Application Policy Infrastructure Controller ( APIC )	<a href="#">0.CSCuy54481</a>	
Cisco Cloupia Unified Infrastructure Controller	<a href="#">0.CSCuy54478</a>	該当するバージョンは5.5リリースで更新されます。
Cisco Digital Media Manager	<a href="#">0.CSCuy54532</a>	5.3 ( 2016年4月28日 ) 5.3.6 ( 2016年4月28日 ) 5.3.6(RB1) ( 2016年4月28日 ) 5.3.6(RB2) ( 2016年4月28日 ) 5.4 ( 2016年4月28日 ) 5.4.1 ( 2016年4月28日 ) 5.4.1(RB1) ( 2016年4月28日 ) 5.4.1(RB2) ( 2016年4月28日 )
Cisco MATE Collector	<a href="#">0.CSCuy58728</a>	
Cisco MATE Design	<a href="#">0.CSCuy58728</a>	
Cisco MATE Live	<a href="#">0.CSCuy58728</a>	
Cisco管理アプライアンス(MAP)(*)	<a href="#">0.CSCuy54443</a>	該当するシステムは2016年4月8日にアップデートされる予定です。
Cisco Mobile Wireless Transport Manager	<a href="#">0.CSCuy54523</a>	
Cisco Multicast Manager	<a href="#">0.CSCuy54509</a>	
Cisco NetFlow Generation Appliance	<a href="#">0.CSCuy54519</a>	
Cisco Network Analysis Module	<a href="#">0.CSCuy54516</a>	
Cisco Packet Tracer	<a href="#">0.CSCuy54539</a>	7.0 ( 2016年7月29日 )
Cisco Policy Suite(CPS)	<a href="#">0.CSCuy58727</a>	9.1 ( 2016年4月30日 )
Cisco Prime Access Registrar	<a href="#">0.CSCuy54512</a>	7.1 ( 2016年4月15日 )
Cisco Prime Collaboration Assurance	<a href="#">0.CSCuy54522</a>	
Cisco Prime Collaboration Deployment	<a href="#">0.CSCuy54636</a>	
Cisco Prime Collaboration Provisioning	<a href="#">0.CSCuy54521</a>	影響を受けるバージョンはすべて更新されています。
Cisco Prime Data Center Network Manager ( DCNM )	<a href="#">0.CSCuy54479</a>	10.0(1) (April 2016)
Cisco Prime Home	<a href="#">0.CSCuy54520</a>	
Cisco Prime IP Express(*)	<a href="#">0.CSCuy54514</a>	

Cisco Prime Infrastructure Standalone Plug and Play Gateway	<a href="#">0.CSCuy54517</a>	
Cisco Prime Infrastructure	<a href="#">0.CSCuy54518</a>	
Cisco Prime LAN Management Solution ( LMS - Solaris )	<a href="#">0.CSCuy54508</a>	
Cisco Prime License Manager	<a href="#">0.CSCuy54540</a>	
Cisco Prime Network Registrar(CPNR)(*)	<a href="#">0.CSCuy54510</a>	
Cisco Prime Network Services Controller(*)	<a href="#">0.CSCuy54525</a>	3.4.2 ( 2016年5月30日 )
Cisco Prime Network	<a href="#">0.CSCuy54504</a>	4.3 (July 2016)
Cisco Prime Optical for SPs	<a href="#">0.CSCuy54513</a>	
Cisco Prime Performance Manager	<a href="#">0.CSCuy54505</a>	1.7SP4 ( 2016年4月27日 )
Cisco Prime Security Manager	<a href="#">0.CSCuy54569</a>	9.3.4.5 ( 2016年5月30日 )
Cisco Security Manager	<a href="#">0.CSCuy54524</a>	
Cisco Show and Share ( SnS )	<a href="#">0.CSCuy54542</a>	
Cisco UCS Central	<a href="#">0.CSCuy54500</a>	
Cisco Unified Intelligence Center ( CUIC )	<a href="#">0.CSCuy74294</a>	
Local Collector Appliance ( LCA )	<a href="#">0.CSCuy54701</a>	
StealthWatch FlowCollector NetFlow		
StealthWatch FlowCollector sFlow		
Stealthwatch Identity		
StealthWatch管理コンソール(SMC)		
StealthWatch UDP Director ( 旧フローレプリケーター )		
Routing and Switching - Enterprise and Service Provider		
Cisco 910 Industrial Router	<a href="#">0.CSCuy54697</a>	IR910ではSSLv2が無効になっています。
Cisco ASR 5000 シリーズ	<a href="#">0.CSCuy54436</a>	
Cisco Connected Gridルーター - CGOS (*)	<a href="#">0.CSCuy54477</a>	16.2(00.192) ( 2016年4月7日 )
Cisco Connected Grid ルーター	<a href="#">0.CSCuy54626</a>	該当するシステムはアップグレード済みです。
Cisco IOS Software and Cisco IOS XE Software	<a href="#">0.CSCuy54623</a>	

Cisco IOS XR ソフトウェア	<a href="#">0.CSCuy54527</a>	
Cisco MDS 9000 Series Multilayer Switches	<a href="#">0.CSCuy54488</a>	7.3.1.DX ( 2016年8月 ) 6.2.17 (June 2016) 7.3.1.NX ( 2016年8月 ) 7.0.3.I3 ( 2016年5月 ) 8.3 ( 2016年11月 )
Cisco Nexus 1000V InterCloud(*)	<a href="#">0.CSCuy54485</a>	1.0.1f ( 2016年3月21日 ) 1.0.1h4.4 ( 2016年3月21日 )
Cisco Nexus 1000V シリーズ スイッチ ( ESX )	<a href="#">0.CSCuy54492</a>	5.2(1)SV3(2.0.200) ( 2016年4月5日 )
Cisco Nexus 3000 Series Switches	<a href="#">0.CSCuy54488</a>	7.3.1.DX ( 2016年8月 ) 6.2.17 (June 2016) 7.3.1.NX ( 2016年8月 ) 7.0.3.I3 ( 2016年5月 ) 8.3 ( 2016年11月 )
Cisco Nexus 4000 Series Blade Switches	<a href="#">0.CSCuy54603</a>	4.1(2)E1(1q) ( 2016年6月30日 )
Cisco Nexus 5000 Series Switches	<a href="#">0.CSCuy54488</a>	7.3.1.DX ( 2016年8月 ) 6.2.17 (June 2016) 7.3.1.NX ( 2016年8月 ) 7.0.3.I3 ( 2016年5月 ) 8.3 ( 2016年11月 )
Cisco Nexus 6000 Series Switches	<a href="#">0.CSCuy54488</a>	7.3.1.DX ( 2016年8月 ) 6.2.17 (June 2016) 7.3.1.NX ( 2016年8月 ) 7.0.3.I3 ( 2016年5月 ) 8.3 ( 2016年11月 )
Cisco Nexus 7000 Series Switches	<a href="#">0.CSCuy54488</a>	7.3.1.DX ( 2016年8月 ) 6.2.17 (June 2016) 7.3.1.NX ( 2016年8月 ) 7.0.3.I3 ( 2016年5月 ) 8.3 ( 2016年11月 )
Cisco Nexus 9000 (ACI/Fabric Switch)	<a href="#">0.CSCuy54484</a>	2.0.1x ( 2016年6月 )
Cisco Nexus 9000シリーズ ( スタンドアロン、NX-OSを実行 )	<a href="#">0.CSCuy57853</a>	7.0(3)I4(1) ( 2016年3月25日 ) 7.0(3)I4(0.42) ( 2016年3月25日 )
Cisco ONS 15454シリーズマルチサービスプロビジョニングプラットフォーム(*)	<a href="#">0.CSCuy54696</a>	



Cisco OnePK All-in-One VM	<a href="#">0.CSCuy54577</a>	
Cisco Service Control Operating System	<a href="#">0.CSCuy54627</a>	
ルーティングおよびスイッチング - スモール ビジネス		
Cisco Sx220スイッチ	<a href="#">0.CSCuy54591</a>	1.4.5.1 (May 2016)
Cisco Sx300スイッチ	<a href="#">0.CSCuy54592</a>	1.4.5.1 (May 2016)
Cisco Sx500スイッチ	<a href="#">0.CSCuy54593</a>	1.4.5.1 (May 2016)
Unified Computing		
Cisco Common Services Platform Collector	<a href="#">0.CSCuy54437</a>	Affected systems have been updated.
Cisco Standalone ラック サーバ CIMC	<a href="#">0.CSCuy54501</a>	
Cisco Unified Computing System (Management software)	<a href="#">0.CSCuy54576</a>	
Cisco Unified Computing System Bシリーズ ( ブレード ) サーバ(*)	<a href="#">0.CSCuy54499</a>	2.2(3d)以降は該当しません。Bシリーズサーバの場合は、このバージョン以降にアップグレードしてください。
Cisco Virtual Security Gateway	<a href="#">0.CSCuy54497</a>	
音声およびユニファイド コミュニケーション デバイス		
Cisco 190 ATA Series Analog Terminal Adaptor	<a href="#">0.CSCuy54633</a>	
Cisco ATA 187 Analog Telephone Adaptor	<a href="#">0.CSCuy54665</a>	
Cisco Agent Desktop for Cisco Unified Contact Center Express	<a href="#">0.CSCuy54639</a>	
Cisco Agent Desktop	<a href="#">0.CSCuy54687</a>	
Cisco Computer Telephony Integration Object Server ( CTIOS )	<a href="#">0.CSCuy54688</a>	
Cisco Emergency Responder	<a href="#">0.CSCuy54646</a>	
Cisco Finesse	<a href="#">0.CSCuy54645</a>	
Cisco Hosted Collaboration Mediation Fulfillment	<a href="#">0.CSCuy54652</a>	
Cisco IM and Presence Service ( CUPS )	<a href="#">0.CSCuy54649</a>	
Cisco IP Interoperability and Collaboration System (IPICS)	<a href="#">0.CSCuy54549</a>	

Cisco Jabber for iOS	<a href="#">0.CSCuy54655</a>	
Cisco MediaSense	<a href="#">0.CSCuy54668</a>	
Cisco Packaged Contact Center Enterprise	<a href="#">0.CSCuy54689</a>	
Cisco Paging Server ( Informacast )	<a href="#">0.CSCuy54654</a>	
Cisco Paging Server	<a href="#">0.CSCuy54654</a>	
Cisco SPA112 2-Port Phone Adapter	<a href="#">0.CSCuy54587</a>	
Cisco SPA122 ATA with Router	<a href="#">0.CSCuy54587</a>	
Cisco SPA232D Multi-Line DECT ATA	<a href="#">0.CSCuy54587</a>	
Cisco SPA30X Series IP Phones	<a href="#">0.CSCuy54590</a>	
Cisco SPA50X Series IP Phones	<a href="#">0.CSCuy54590</a>	
Cisco SPA51X Series IP Phones	<a href="#">0.CSCuy54590</a>	
Cisco SPA525G	<a href="#">0.CSCuy54588</a>	
Cisco TAPI Service Provider ( TSP )	<a href="#">0.CSCuy54635</a>	
Cisco Unified 6901 IP フォン	<a href="#">0.CSCuy54661</a>	
Cisco Unified 6945 IP フォン	<a href="#">0.CSCuy54666</a>	
Cisco Unified 7800 Series IP Phones	<a href="#">0.CSCuy54672</a>	
Cisco Unified 8831 シリーズ IP Conference Phone	<a href="#">0.CSCuy54663</a>	
Cisco Unified 8945 IP フォン	<a href="#">0.CSCuy54662</a>	
Cisco Unified 8961 IP フォン	<a href="#">0.CSCuy54651</a>	
Cisco Unified 9951 IP フォン	<a href="#">0.CSCuy54651</a>	
Cisco Unified 9971 IP フォン	<a href="#">0.CSCuy54651</a>	
Cisco Unified Attendant Console Advanced	<a href="#">0.CSCuy54630</a>	
Cisco Unified Attendant Console Business Edition	<a href="#">0.CSCuy54630</a>	
Cisco Unified Attendant Console Department Edition	<a href="#">0.CSCuy54630</a>	
Cisco Unified Attendant Console Enterprise Edition	<a href="#">0.CSCuy54630</a>	

Cisco Unified Attendant Console Premium Edition	<a href="#">0.CSCuy54630</a>	
Cisco Unified Attendant Console Standard	<a href="#">0.CSCuy54631</a>	
Cisco Unified Communications Domain Manager	<a href="#">0.CSCuy54640</a>	11.5.1 ( 2016年8月 )
Cisco Unified Communications Manager ( UCM )	<a href="#">0.CSCuy54634</a>	
Cisco Unified Communications Manager Session Management Edition ( SME )	<a href="#">0.CSCuy54634</a>	
Cisco Unified Communications for Microsoft Lync	<a href="#">0.CSCuy54641</a>	
Cisco Unified Contact Center Enterprise	<a href="#">0.CSCuy54688</a>	
Cisco Unified Contact Center Express	<a href="#">0.CSCuy74300</a>	
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	<a href="#">0.CSCuy54629</a>	
Cisco Unified IP Phone 7900 Series	<a href="#">0.CSCuy54674</a>	
Cisco Unified Intelligent Contact Management Enterprise	<a href="#">0.CSCuy54688</a>	
Cisco Unified Wireless IP Phone	<a href="#">0.CSCuy54681</a>	SSLv2は無効です。
Cisco Unified Workforce Optimization	<a href="#">0.CSCuy54680</a>	WFO 10.5 ( 2016年3月31日 ) WFO 11.0 ( 2016年4月15日 )
Cisco Unity Connection ( UC )	<a href="#">0.CSCuy54637</a>	
Cisco Virtualization Experience Media Engine	<a href="#">0.CSCuy54679</a>	11.7 ( 2016年7月28日 )
<b>ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス</b>		
Cisco AnyRes Live ( CAL )	<a href="#">0.CSCuy54616</a>	9.6.4 (April 2016)
Cisco DCM Series 9900-Digital Content Manager	<a href="#">0.CSCuy54502</a>	
Cisco Digital Media Players (DMP) 4300 Series	<a href="#">0.CSCuy54531</a>	5.4(1) ( 2016年4月10日 )
Cisco Digital Media Players (DMP) 4400 Series	<a href="#">0.CSCuy54531</a>	5.4(1) ( 2016年4月10日 )
Cisco Edge 300 Digital Media Player	<a href="#">0.CSCuy54698</a>	1.6RB4_4 ( 2016年4月15日 )

Cisco Edge 340 Digital Media Player	<a href="#">0.CSCuy54700</a>	該当するシステムは、2016年4月15日までにアップデートされる予定です。
Cisco Enterprise Content Delivery System (ECDS)	<a href="#">0.CSCuy54533</a>	2.6.7 ( 2016年4月15日 )
Cisco Expresswayシリーズ(*)	<a href="#">0.CSCuy54547</a>	
シスコヘッドエンドシステムリリース(*)	<a href="#">0.CSCuy54611</a>	1.06 ( 2016年5月1日 ) 1.1.3 ( 2016年5月1日 ) 2.0.10 ( 2016年5月1日 ) 2.1.2 ( 2016年5月1日 ) 3.0.4 ( 2016年5月1日 )
Cisco Media Experience Engines(MXE)(*)	<a href="#">0.CSCuy54538</a>	
Cisco Media Services Interface	<a href="#">0.CSCuy54528</a>	
Cisco Model D9485 DAVIC QPSK (*)	<a href="#">0.CSCuy54612</a>	1.2.4 ( 2016年8月31日 )
Cisco TelePresence 1310(*)	<a href="#">0.CSCuy54628</a>	
Cisco TelePresence Conductor	<a href="#">0.CSCuy54529</a>	SSLv2は、ソフトウェアバージョンXC4.0以降では無効になっています。
Cisco TelePresence Content Server ( TCS )	<a href="#">0.CSCuy54545</a>	
Cisco TelePresence ISDN GW 3241	<a href="#">0.CSCuy54534</a>	
Cisco TelePresence ISDN GW MSE 8321	<a href="#">0.CSCuy54534</a>	
Cisco TelePresence ISDN Link	<a href="#">0.CSCuy54535</a>	
Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)	<a href="#">0.CSCuy54536</a>	
Cisco TelePresence Serial Gateway Series	<a href="#">0.CSCuy54541</a>	
Cisco TelePresence Server 8710, 7010	<a href="#">0.CSCuy54546</a>	
Cisco TelePresence Server on Multiparty Media 310、 320	<a href="#">0.CSCuy54546</a>	
Cisco TelePresence Server on Virtual Machine	<a href="#">0.CSCuy54546</a>	
Cisco TelePresence Supervisor MSE 8050	<a href="#">0.CSCuy54537</a>	
Cisco TelePresenceシステム1000(*)	<a href="#">0.CSCuy54628</a>	

Cisco TelePresenceシステム1100(*)	<a href="#">0.CSCuy54628</a>	
Cisco TelePresenceシステム1300(*)	<a href="#">0.CSCuy54628</a>	
Cisco TelePresence System 3000シリーズ(*)	<a href="#">0.CSCuy54628</a>	
Cisco TelePresenceシステム500-32(*)	<a href="#">0.CSCuy54628</a>	
Cisco TelePresenceシステム500-37(*)	<a href="#">0.CSCuy54628</a>	
Cisco TelePresence TX 9000シリーズ(*)	<a href="#">0.CSCuy54628</a>	
Cisco TelePresence Video Communication Server(VCS)(*)	<a href="#">0.CSCuy54547</a>	
Cisco VEN501 Wireless Access Point	<a href="#">0.CSCuy54550</a>	
Cisco Video Distribution Suite for Internet Streaming ( VDS-IS/CDS-IS )	<a href="#">0.CSCuy54553</a>	4.3.2 (May 2016)
Cisco Video Surveillance 3000 Series IP Cameras	<a href="#">0.CSCuy54583</a>	
Cisco Video Surveillance 3000 Series IP Cameras	<a href="#">0.CSCuy54584</a>	SSLv2はサポートされていません。
Cisco Video Surveillance 4000 Series High-Definition IP Cameras	<a href="#">0.CSCuy54580</a>	
Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras	<a href="#">0.CSCuy54581</a>	
Cisco Video Surveillance 6000 Series IP Cameras	<a href="#">0.CSCuy54583</a>	
Cisco Video Surveillance 6000 Series IP Cameras	<a href="#">0.CSCuy54584</a>	SSLv2はサポートされていません。
Cisco Video Surveillance 7000 Series IP Cameras	<a href="#">0.CSCuy54583</a>	
Cisco Video Surveillance 7000 Series IP Cameras	<a href="#">0.CSCuy54584</a>	SSLv2はサポートされていません。
Cisco Video Surveillance Media Server	<a href="#">0.CSCuy54585</a>	7.8 ( 2016年7月1日 )
Cisco Video Surveillance PTZ IP	<a href="#">0.CSCuy54583</a>	

Cameras		
Cisco Video Surveillance PTZ IP Cameras	<a href="#">0.CSCuy54584</a>	SSLv2はサポートされていません。
Cisco Videoscape Control Suite	<a href="#">0.CSCuy54551</a>	3.6.0 ( 2016年4月30日 )
クラウドオブジェクトストア(COS) (*)	<a href="#">0.CSCuy54552</a>	3.8.0 ( 2016年3月30日 )
Tandberg Codian ISDN GW 3210/3220/3240	<a href="#">0.CSCuy54534</a>	
Tandberg Codian MSE 8320 model	<a href="#">0.CSCuy54534</a>	
ワイヤレス		
Cisco Aironet 2700 シリーズ アクセ ス ポイント	<a href="#">0.CSCuy54506</a>	
Cisco Mobility Services Engine ( MSE )	<a href="#">0.CSCuy58090</a>	
CiscoワイヤレスLANコントローラ (WLC)(*)	<a href="#">0.CSCuy58091</a>	8.0 (April 2016) 8.3 (May 2016)
シスコ ホステッド サービス		
Cisco Intelligent Automation for Cloud	<a href="#">0.CSCuy54548</a>	
Cisco Proactive Network Operations Center	<a href="#">0.CSCuy54441</a>	
Cisco Registered Envelope Service ( CRES )	<a href="#">0.CSCuy54451</a>	
Cisco Services Provisioning Platform ( SPP )	<a href="#">0.CSCuy54682</a>	
Cisco Smart Care	<a href="#">0.CSCuy54565</a>	
Cisco Universal Small Cell 5000 シ リーズ ( V3.4.2.x ソフトウェアを実 行 )	<a href="#">0.CSCuy54610</a>	
Cisco Universal Small Cell 7000 シ リーズ ( V3.4.2.x ソフトウェアを実 行 )	<a href="#">0.CSCuy54610</a>	
Cisco Universal Small Cell usc-juh	<a href="#">0.CSCuy54608</a>	
Cisco WebEx Connect クライアン ト ( Windows )	<a href="#">0.CSCuy54465</a>	
Cisco WebEx Meeting Center	<a href="#">0.CSCuy54473</a>	
Cisco WebEx Meetings (Meeting	<a href="#">0.CSCuy54472</a>	

Center, Training Center, Event Center, Support Center)		
Cisco WebEx Messenger Service	<a href="#">0.CSCuy54466</a>	
Network Health Framework (NHF)	<a href="#">0.CSCuy54702</a>	
Network Performance Analytics (NPA)	<a href="#">0.CSCuy54703</a>	
Partner Supporting Service ( PSS ) 1.x	<a href="#">0.CSCuy54568</a>	
Serial Number Assessment Service ( SNAS )	<a href="#">0.CSCuy54571</a>	
Services Analytic Platform	<a href="#">0.CSCuy54445</a>	
Small Cell factory recovery root filesystem V2.99.4 or later	<a href="#">0.CSCuy54607</a>	

## 脆弱性を含んでいないことが確認された製品

シスコは、このアドバイザリに記載された脆弱性が次のシスコ製品には影響を与えないことを確認しました。

### エンドポイント クライアントとクライアント ソフトウェア

- Cisco WebEx Meetings for BlackBerry
- Cisco WebEx Productivity Tools

### ネットワークおよびコンテンツ セキュリティ デバイス

- Cisco ASA Content Security and Control ( CSC ) Security Services Module

### ネットワーク管理とプロビジョニング

- Cisco Configuration Professional
- Cisco Prime LAN Management Solution ( LMS - WindowsおよびLinux )
- Cisco Prime Network Registrar IP アドレス マネージャ ( IPAM )

### Routing and Switching - Enterprise and Service Provider

- Cisco Broadband Access Center Telco Wireless
- Cisco IOS XE ( SSL VPN 機能 )

## 音声およびユニファイド コミュニケーション デバイス

- Cisco 7937 IP Phone
- Cisco 8800 Series IP Phones - VPN Feature
- Cisco DX シリーズ IP フォン
- Cisco Remote Silent Monitoring
- Cisco SPA8000 8ポートIPテレフォニーゲートウェイ
- Cisco SPA8800 IP テレフォニーゲートウェイ ( 4 FXS ポートと 4 FXO ポートを内蔵 )
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified Sip Proxy
- Cisco Unified Web Interaction Manager
- Cisco Virtual PGW 2200 ソフトスイッチ
- Cisco Voice Portal ( CVP )

## ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス

- Cisco AnyRes VOD ( CAL )
- Cisco D9859 Advanced Receiver Transcoder
- Cisco TelePresence EX Series
- Cisco TelePresence MX Series
- Cisco TelePresence Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence Integrator C Series

## シスコ ホステッド サービス

- Cisco Cloud Web Security
- Cisco Connected Analytics For Collaboration
- Cisco One Portal
- Cisco SmartConnection
- Cisco SmartReports
- Cisco Unified Services Delivery Platform ( CUSDP )
- コミュニケーション/コラボレーションサイジングツール、仮想マシン配置ツール、Cisco Unified Communications Upgrade Readiness Assessment
- Life Cycle Management Agent Manager ( LCM )

## 詳細

2016年3月1日にOpenSSL Software Foundationのセキュリティアドバイザリで公開された脆弱性の名前とそれに関連するCommon Vulnerabilities and Exposures(CVE)IDは次のとおりです。



## マルチベンダーSSL/TLS実装におけるDROWN情報漏えいの脆弱性

SSL/TLSを使用する複数のベンダー製品の脆弱性により、認証されていないリモートの攻撃者がDecrypting RSA with Obsolete and Weaked eEncryption(DROWN)クロスプロトコル攻撃を実行し、機密情報にアクセスする可能性があります。

この脆弱性は、Transport Layer Security(TLS)内で脆弱なRivest, Shamir, and Adleman(RSA)暗号スイートの使用を可能にする可能性があるSSLv2プロトコルの実装エラーに起因します。攻撃者は、ターゲットシステムと、同じ秘密キーを使用して接続の1つを監視し、場合によっては復号化する脆弱なSSLv2サーバ間のトラフィックを傍受することで、この脆弱性を不正利用する可能性があります。攻撃者は、復号化された暗号文をターゲットサーバに返し、サーバの応答から判断して、暗号化された通信で使用される秘密鍵を決定する可能性があります。この不正利用により、攻撃者はターゲットクライアントとSSLv2サーバ間のTLSセッションを復号化でき、機密情報へのアクセスに利用される可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0800です。

## OpenSSL Bleichenbacher保護のセキュリティバイパスの脆弱性

OpenSSLでのSSLv2プロトコルの実装における脆弱性により、認証されていないリモートの攻撃者がセキュリティ制限をバイパスできる可能性があります。

この脆弱性は、該当ソフトウェアによるエクスポート暗号スイートに対するBleichenbacher保護の不適切な実装に起因します。攻撃者は、この脆弱性を不正利用してBleichenbacher oracleを確立し、Obsolete and Weaked eEncryption(DROWN)攻撃を使用した復号化RSAのより多くのクライアントの実行を支援する可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0704です。

## OpenSSL SSLv2のマスターキーの回復情報漏えいの脆弱性

OpenSSLの脆弱性により、認証されていないリモートの攻撃者が機密情報にアクセスできる可能性があります。

この脆弱性は、影響を受けるソフトウェアによって実装されたセキュリティ制限が不適切であることに起因します。認証されていないリモートの攻撃者が、通信トラフィックを傍受することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はターゲットシステムの機密情報にアクセスできる可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0703です。

## OpenSSLデジタル署名アルゴリズムの秘密キー処理における二重解放の脆弱性

OpenSSL の脆弱性により、認証されていないリモート攻撃者がサービス妨害 ( DoS ) 状態を発生させる可能性があります。

この脆弱性は、該当ソフトウェアによる不正なデジタル署名アルゴリズム(DSA)秘密キーの不適切な解析に起因します。攻撃者は、不正な形式のDSA秘密キーをアプリケーションと交換しようとする試みで、脆弱なバージョンのOpenSSLを使用するアプリケーションのユーザを誘導して攻撃者によって制御されるサーバに接続させることで、この脆弱性を不正利用する可能性があります。この不正利用により、メモリの二重空き状態が引き起こされ、攻撃者はこれを利用してDoS状態を引き起こす可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0705です。

OpenSSL SRP\_VBASE\_get\_by\_userメソッドのメモリリークの脆弱性

OpenSSL の脆弱性により、認証されていないリモート攻撃者がサービス妨害 ( DoS ) 状態を発生させる可能性があります。

この脆弱性は、不適切なメモリ処理に起因します。認証されていないリモートの攻撃者は、悪意のあるログイン要求をSRPユーザデータベースに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は該当システムでメモリリークを引き起こし、その結果DoS状態が発生する可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0798です。

OpenSSL BN\_hex2bnおよびBN\_dec2bn関数NULLポインタ逆参照の脆弱性

OpenSSL の脆弱性により、認証されていないリモート攻撃者がサービス妨害 ( DoS ) 状態を発生させる可能性があります。

この脆弱性は、該当ソフトウェアによる不適切なメモリ操作に起因します。認証されていないリモートの攻撃者は、巧妙に細工された入力を送信して該当ソフトウェアで処理することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はアプリケーションを断続的に停止させ、DoS状態を引き起こす可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0797です。

OpenSSL BIO\_\*printf関数の範囲外のメモリ読み取りの脆弱性

OpenSSLの脆弱性により、認証されていないリモートの攻撃者が機密情報にアクセスできる可能性があります。

この脆弱性は、影響を受けるソフトウェアによって実行される境界チェックが不適切であることに起因します。認証されていないリモートの攻撃者は、巧妙に細工された入力を送信して該当ソフトウェアで処理することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はターゲットシステムの機密情報にアクセスできる可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0799およびCVE-2016-2842です。

### OpenSSL RSA暗号化キー回復の脆弱性

OpenSSLの脆弱性により、認証されていないローカルの攻撃者が機密情報にアクセスできる可能性があります。

この脆弱性は、該当ソフトウェアによる不適切なメモリ管理に起因します。認証されていないローカルの攻撃者が、該当ソフトウェアに悪意のあるコードを挿入することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はターゲットシステムの機密情報にアクセスできる可能性があります。

本脆弱性のIDはCVE ID CVE-2016-0702です。

## 回避策

回避策は今後 Cisco bugs に記載され、Cisco Bug Search Tool を使用して検索可能です。

## 修正済みソフトウェア

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リリースしています。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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ 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、お客様は以下のリンクに記載された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。

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN .html>

また、お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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 and Responses アーカイブ](#)や[後続のアドバイザリ](#)を参照して、[侵害を受ける可能性と完全な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、および現在のハードウェアとソフトウェアの構成は新規リリースでも継続して適切なサポートが受けられることを確認してください。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。

サービス契約をご利用でないお客様

シスコから直接購入したが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、サードパーティベンダーから購入したが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を入手してください。

[http://www.cisco.com/c/ja\\_jp/support/web/tsd-cisco-worldwide-contacts.html](http://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html)

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。

## 推奨事項

`$propertyAndFields.get("recommendations")`

## 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エクスプロイト事例を確認していません。

## 出典

これらの脆弱性は、2016年3月1日に [OpenSSL Software Foundation](#) によって [公開](#)されました。

DROWN攻撃は、Nimrod Aviram、Sebastian Schinzel、Juraj Somorovsky、Nadia Heninger、Maik Dankel、Jens Steube、Luke Valenta、Shaanan Cohney、Susanne Engels、Christof Paar、およびYuval ShavittによってCisco PSIRTに個別に報告されました。シスコは、攻撃を報告していただき、攻撃の開示に協力していただいたことに対して、お礼を申し上げます。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
2.2	脆弱性のある製品のリストを更新。	「該当製品」、「脆弱性のある製品」	Interim	2016年5月23日
2.1	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年5月11日
2.0	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年5月2日
1.9	調査中または脆弱性のある製品のリストを更新。	「該当製品」、「脆弱性のある製品」	Interim	2016年4月11日
1.8	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年4月1日
1.7	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年3月18日
1.6	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年3月15日
1.5	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年3月10日
1.4	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年3月9日
1.3	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年3月8日
1.2	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年3月4日
1.1	調査中の製品、脆弱性のある製品、脆弱性を含まない製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含まないことが確認された製品	Interim	2016年3月3日

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Interim	2016年3月2日

## 利用規約

本アドバイザー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も示唆するものではありません。本アドバイザー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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。