Vulnerability in Samba Affecting Cisco Products: May 2017

High

アドバイザリーID : cisco-sa-20170530-samba

初公開日 : 2017-05-30 19:30

最終更新日 : 2017-07-11 13:47

バージョン 1.5 : Final

回避策 : Yes

Cisco バグ ID :

CVE-2017-7494

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

2017 年 5 月 24 日、Samba チームは、認証された攻撃者がターゲット システム上で任意のコードをリモートで実行できる Samba サーバ ソフトウェアの脆弱性を公開しました。

本脆弱性の ID は CVE ID CVE-2017-7494 です。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170530-samba

影響を受ける製品

シスコでは、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、製品ラインを調査しました。 製品が影響を受けているかについて情報に関してはこのアドバイザリの 脆弱性が存在する製品および 脆弱性が存在しない製品セクションを参照して下さい。

脆弱性が存在する製品 セクションは各々の影響を受けた製品のための Cisco バグ ID が含まれています。 バグは Ciscoバグ 検索ツールを通してアクセス可能で、回避策 (もし可能であれば) および修正済みソフトウェアリリースを含む追加プラットフォーム別の情報が、含まれています。

脆弱性が存在する製品

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

Product	Cisco Bug ID	Fixed Release Availability
Network Management and Provisioning		
Cisco Network Analysis Module	CSCve61674	

Video, Streaming, TelePresence, and Transcoding Devices		
Cisco MXE 3500 Series Media Experience Engines	CSCve61675	Patch for 3.5.2 (17-Jul-2017)
Cisco Video Surveillance Media Server	CSCve61680	10.0.0 (October 2017)

脆弱性が存在しない製品

シスコは製品ラインを調査し、この脆弱性の影響を受ける可能性のある製品と、それぞれの影響内容を割り出しました。 シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

Network Application, Service, and Acceleration

- Cisco Application and Content Networking System（ACNS）
- Cisco Wide Area Application Services（WAAS）

Network and Content Security Devices

- Cisco コンテンツ セキュリティ管理アプライアンス
- Cisco Identity Services Engine（ISE）
- Cisco Web Security Appliance (WSA)

Network Management and Provisioning

- Lancope Stealthwatch Endpoint Concentrator
- Lancope Stealthwatch FlowCollector NetFlow
- Lancope Stealthwatch FlowCollector sFlow
- Lancope Stealthwatch FlowSensor
- Lancope Stealthwatch SMC
- Lancope Stealthwatch UDP Director

Routing and Switching - Small Business

- Cisco Small Business RV シリーズ RV320 デュアル ギガビット WAN VPN ルータ

Unified Computing

- Cisco Common Services Platform Collector

Voice and Unified Communications Devices

- Cisco IP Interoperability and Collaboration System (IPICS)

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco Digital Media Manager

- Cisco Expressway Series
- Cisco TelePresence Video Communication Server（VCS）
- Cisco VDS Recorder
- Cisco VDS-TV Caching Nodes
- Cisco VDS-TV Streamer
- Cisco VDS-TV Vault

細部

Samba の脆弱性により、認証されたリモート攻撃者が任意のコードを実行する可能性があります。

この脆弱性の原因は、該当ソフトウェアでのユーザ入力の検証が不十分なことにあります。 ターゲット システムの書き込み可能な共有領域へのアクセス権を持つ攻撃者は、書き込み可能な共有領域に悪意のある共有ライブラリをアップロードする可能性があります。 ターゲット システムによって悪意のある共有ライブラリが読み込まれて実行されると、攻撃者は任意のコードを実行し、これを使用してさらなる攻撃を行う可能性があります。

回避策

どの回避策でも、もし可能であれば、 Ciscoバグ 検索ツールを通してアクセス可能であるCiscoバグで文書化されています。

固定ソフトウェア

シスコがリリースした無償ソフトウェア アップデートをインストールしたり、関連する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、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 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際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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 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

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。

修正済みリリース

脆弱性が存在する各製品に対して、影響を受けるリリースと修正済みリリースを確認するには、製品によって特定される Cisco Bug を参照してください。 これらのバグはこのアドバイザリの脆弱性が存在する製品 セクションの表にリストされています。 Ciscoバグは Ciscoバグ 検索ツール を通してアクセス可能です。

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やその公表を確認していません。

ソース

この脆弱性は、Samba チームにより発見され、次の URL で公開されました。
https://www.samba.org/samba/security/CVE-2017-7494.html

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170530-samba

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.5	脆弱性が存在しない製品のリストを更新。 これで製品ラインの調査が完了したことを示す。	「影響を受ける製品」、「脆弱性が存在しない製品」、「修正済みリリース」	最終版	2017 年 7 月 11 日
1.4	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	最終版	2017-July-07
1.3	Updated product lists.	Affected Products, Vulnerable Products,	Interi	2017-

		Products Confirmed Not Vulnerable	m	June-12
1.2	Updated product lists.	Affected Products, Products Confirmed Not Vulnerable	Interim	2017-June-02
1.1	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-June-01
1.0	初回公開リリース		Interim	2017-May-30

利用規約