Cisco Unified Communications Domain Manager におけるリモート コード実行の脆弱性

Critical

アドバイザリーID : cisco-sa-20180221-ucdm

初公開日 : 2018-02-21 16:00

最終更新日 : 2018-03-09 14:47

バージョン 1.1 : Final

CVSSスコア : 9.8

回避策 : No workarounds available

Cisco バグ ID : CSCvi10692 CSCuv67964

CVE-2018-0124

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

Cisco Unified Communications Domain Manager の脆弱性により、未認証のリモート攻撃者がセキュリティ保護をバイパスし、権限を昇格させ、任意のコードを実行する可能性があります。

この脆弱性は、アプリケーション設定時における安全でないキー生成に起因します。 この脆弱性は、安全でないキーを使用して攻撃者がターゲット アプリケーションに任意の要求を送信し、安全でない既知のキー値を使用してセキュリティ保護をバイパスすることによって、不正利用される可能性があります。 不正利用されると、攻撃者に任意のコードを実行される可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

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-20180221-ucdm

該当製品

脆弱性のある製品

この脆弱性は、Cisco Unified Communications Domain Manager リリース 11.5(2) より前（Cisco Unified Communications Domain Manager Classic リリース 8.1.9 以前を含む）に影響

を与えます。

デバイスで実行中のソフトウェア リリースを確認するには、デバイスの CLI で管理者権限で **app status** コマンドを実行します。 CLI コマンドの出力は、次の例のようになります。

```
platform@CUCDM-11-5-1:~$ app status
selfservice v11.5.1 (2017-05-22 14:39)
|-node running
voss-deviceapi v11.5.1 (2017-05-22 14:39)
|-voss-cnf_collector running
|-voss-wsgi running
|-voss-queue running
cluster v11.5.1 (2017-05-22 14:34)
template_runner v0.0.0
mongodb v11.5.1 (2017-05-22 14:36)
|-arbiter running
|-database running
support v11.5.1 (2017-05-22 14:36)
snmp v11.5.1 (2017-05-22 14:36)
|-daemon running (completed)
|-traps running (completed)
platform v11.5.1 (2017-05-22 14:37)
nginx v11.5.1 (2017-05-22 14:36)
|-proxy running
services v11.5.1 (2017-05-22 14:34)
|-wsgi running
|-logs running
|-firewall running
|-mount running
|-scheduler running
|-syslog running (completed)
|-time running (completed)
security v11.5.1 (2017-05-22 14:37)
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

回避策

この脆弱性に対処する回避策はありません。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.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。

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。
https://www.cisco.com/c/en/us/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

この脆弱性は、Cisco Unified Communications Domain Manager リリース 11.5(2) 以降で修正されています。

このソフトウェアは Cisco.com の Software Center からダウンロードできます。ダウンロードするには、[製品（Products）] > [ユニファイドコミュニケーション（Unified Communications）] > [コール制御（Call Control）] > [ホステッドコラボレーション（Hosted Collaboration）] > [Hosted Collaboration Solution (HCS)] > [Hosted Collaboration Solutionバージョン 11.5（Hosted Collaboration Solution Version 11.5）] > [Unified Communications Domain Manager（CUCDM）アップデート-11.5(2)（Unified Communications Domain Manager (CUCDM) Updates-11.5(2)）] の順にアクセスします。

Cisco Unified Communications Domain Manager Classic リリース 8.1(9) ER1 のパッチは、Cisco.com の Software Center からダウンロードできます。ダウンロードするには、**[製品（Products）] > [ユニファイドコミュニケーション（Unified Communications）] > [コール制御（Call Control）] > [ホステッドコラボレーション（Hosted Collaboration）] > [Hosted Collaboration Solution (HCS)] > [Hosted Collaboration Solutionバージョン 11.5（Hosted Collaboration Solution Version 11.5）] > [Unified Communications Domain**

Manager（CUCDM）アップデート-8.1.9ER1（Unified Communications Domain Manager (CUCDM) Updates-8.1.9ER1]の順にアクセスします。

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。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180221-ucdm

改訂履歴

Version	Description	Section	Status	日付
1.1	影響を受けるソフトウェア、および Cisco UCDM リリース 8 の情報に関する更新を含む。	該当製品、修正済みソフトウェア	Final	2018 年 3 月 9 日
1.0	初回公開リリース		Final	2018 年 2 月 21 日

利用規約