

Cisco HyperFlex ソフトウェアの静的署名キーの脆弱性

High

アドバイザーID : cisco-sa-20181003-hyperflex-secret

初公開日 : 2018-10-03 16:00

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvj95632](#)

[CSCvk22858](#)

[CVE-2018-15382](#)

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 HyperFlex ソフトウェアの脆弱性により、認証されていないリモートの攻撃者が有効な署名付きセッショントークンを生成する可能性があります。

この脆弱性は、1つの静的署名キーがすべての Cisco HyperFlex システムに存在するために発生します。攻撃者は1つの HyperFlex システムから静的署名キーにアクセスし、そのキーを使用して別の HyperFlex システムの有効な署名付きセッショントークンを生成することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功した攻撃者は、権限を持たないシステムの HyperFlex Web UI にアクセスす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。

このアドバイザーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-hyperflex-secret>

該当製品

脆弱性のある製品

この脆弱性は、3.5(1a) より前の Cisco HyperFlex ソフトウェア リリースに影響を及ぼします。

HyperFlex ソフトウェア リリースの確認

インストールされている Cisco HyperFlex ソフトウェアのリリースを確認するために、管理者は CLI または GUI を使用できます。

CLI を使用する場合、管理者は `stcli about` コマンドを発行できます。デバイスが Cisco HyperFlex ソフトウェア リリース 3.0(1d) を実行している場合、コマンドの出力例は次のようになります。

```
root@hxcluster:~# stcli about
serviceType: stMgr
instanceUuid: c4f0441c-xxxx-xxxx-xxxx-xxxxxxxxxxxx name: HyperFlex StorageController locale:
English (United States) serialNumber: WZP#####OCD,WZP#####OG9,WZP##### apiVersion: 0.1
modelName: HX240C-M5L build: 3.0.1d-29754 (internal) displayVersion: 3.0(1d)
fullName: HyperFlex StorageController 3.0.1d
productVersion: 3.0.1d-29754
```

GUI を使用する場合、管理者は HXConnect にログイン後、ページの左下にある [バージョン情報 (About)] リンクをクリックできます。

脆弱性を含んでいないことが確認された製品

このアドバイザリの [脆弱性が存在する製品の](#) セクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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 HyperFlex 3.5(1a) で修正されています。

ソフトウェア アップデートは、Cisco.com の [Software Center](#) から次の手順でダウンロードできます。

1. [すべて参照 (Browse all)] をクリックします。
2. [ハイパーコンバージド インフラストラクチャ (Hyperconverged Infrastructure)] > [HyperFlex HX データ プラットフォーム (HyperFlex HX Data Platform)] を選択します。
3. [HyperFlex HX データ プラットフォーム (HyperFlex HX Data Platform)] ページの左側のペインを使用して各リリースにアクセスします。

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-20181003-hyperflex-secret>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018年10月3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。