Cisco HyperFlex ソフトウェアの認証されていないルート アクセスによる脆弱性

High

アドバイザリーID : cisco-sa-20190220-chn-root-access

初公開日 : 2019-02-20 16:00

最終更新日 : 2019-04-04 18:44

バージョン 1.1 : Final

CVSSスコア : 8.1

回避策 : Yes

Cisco バグ ID : CSCvk31047

CVE-2019-1664

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 *hxterm* サービスの脆弱性により、認証されていないローカルの攻撃者がクラスタ内のすべてのノードに対する*ルート アクセス*を取得する可能性があります。

この脆弱性は、認証の管理が不十分であることに起因します。 攻撃者は、権限のないローカル ユーザとして *hxterm* サービスに接続することにより、この脆弱性をエクスプロイトします。 エクスプロイトに成功すると、攻撃者は HyperFlex クラスタのすべてのメンバー ノードに対する*ルート アクセス*を取得できる可能性があります。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。 本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-chn-root-access

該当製品

脆弱性のある製品

この脆弱性は、3.5(2a) 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
modelNumber: 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 HX Connect 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

修正済みリリースにアップグレードできないお客様に使用可能な、この脆弱性の回避策があります。 回避策の実装の調整に関しては、 Cisco Technical Assistance Center（TAC）にお問い合わせください。

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。
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(2a) 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-20190220-chn-root-access

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	回避策の可用性を更新しました。	回避策	最終版	2019 年 4 月 4日
1.0	初回公開リリース		最終版	2019 年 2 月 20 日

利用規約