Cisco IoT Field Network Directorにおけるクレデンシャルの保護されていないストレージの脆弱性

Medium	**アドバイザリーID :** cisco-sa-FND-PWH-yCA6M7p **初公開日 :** 2020-11-18 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.1 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvt45257	CVE-2020-26079

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 IoT Field Network Director(FND)のWeb UIの脆弱性により、認証されたリモート攻撃者が該当デバイスのユーザパスワードのハッシュを取得する可能性があります。

この脆弱性は、ユーザクレデンシャルの保護が不十分であることに起因します。攻撃者は、管理ユーザとしてログインし、ユーザ情報のコールを作成することで、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、攻撃者は該当デバイスのユーザパスワードのハッシュ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。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-FND-PWH-yCA6M7p

該当製品

脆弱性のある製品

公開時点では、この脆弱性はリリース4.6.1より前のCisco IoT FNDリリースに影響を与えました。

最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

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のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

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

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ 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アップグレード ソリューション一式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。

修正済みリリース

公開時点で、Cisco IoT FNDリリース4.6.1以降には、この脆弱性に対する修正が含まれています。

最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

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

この脆弱性は、シスコのビリー・ピアスが社内セキュリティテストで発見したものです。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-PWH-yCA6M7p

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース	—	最終版	2020年11月18日

利用規約

本アドバイザリ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。 本アドバイザリ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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、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。