脆弱性をロードする Cisco FindIT 検出 ユーティリティ不確かなライブラリ

Medium	**アドバイザリーID :** cisco-sa-20171115-findit **初公開日 :** 2017-11-15 16:00 **最終更新日 :** 2017-11-15 19:07 **バージョン 1.1 :** Final **CVSSスコア :** 4.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvf37955	CVE-2017-12314

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 FindIT ネットワーク検出ユーティリティの脆弱性は可能性としてはデバイス の アベイラビリティに部分的な影響、機密保持および統合を引き起こす攻撃により、前もって積む DLL を行う認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は期待していた DLL ファイルの代りに仕様の悪意のあるコピーを、nondefined DLL ファイル ロードするアプリケーションが原因です。 攻撃者は上位 システムのサーチ パス内の影響を受けた DLL を置くことによってこの脆弱性を不正利用する可能性があります。 従ってエクスプロイトは攻撃者がシステム、部分的に妥協機密保持、統合およびデバイスでアベイラビリティに悪意のある DLL ファイルをロードすることを可能にする可能性があります。

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-20171115-findit

該当製品

脆弱性のある製品

この脆弱性は Cisco FindIT ネットワーク検出ユーティリティに影響を与えます。 該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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

修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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。

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

Cisco はこの脆弱性を報告するためにステファン Kanthak に感謝することを望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-findit

改訂履歴

Version	Description	Section	Status	日付
1.1	信じられた外部研究者。	Source	Final	2017-November-15
1.0	初回公開リリース		Final	2017-November-15

利用規約

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。