Cisco IoT Field Network Director において、メモリリークにより Denial of Service（DoS）が引き起こされる脆弱性

High

アドバイザリーID : cisco-sa-20170906-fnd

初公開日 : 2017-09-06 16:00

バージョン 1.0 : Final

CVSSスコア : 7.5

回避策 : Yes

Cisco バグ ID : CSCvc77164

CVE-2017-6780

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（IoT-FND）の TCP 制限プロセスにおける脆弱性により、認証されていないリモートの攻撃者がシステムのメモリ資源を消費させ、デバイスを強制的に再起動できる危険性があります。

本脆弱性はレート制限保護が不十分なことに起因します。 標的デバイス上で開放されている特定のリスニング ポートに大量の TCP パケットが送信されると、脆弱性がエクスプロイトされる可能性があります。 エクスプロイトが成功すると、不必要なメモリリークが発生します。 空き容量が一定レベルを切るとシステムが再起動し、一時的なサービス妨害（DoS）状態が発生します。 ただし DoS 状態はデバイスの再起動処理が終了すると解消します。

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-20170906-fnd

該当製品

修正済みソフトウェア

本脆弱性は、以下のシスコ製品に影響します。

- Connected Grid Network Management System（IoT-FND Release 4.0 より前のリリースを実行している場合）
- IoT Field Network Director（IoT-FND リリース 4.0 より前のリリースを実行している場合）

注:「Cisco Connected Grid ネットワーク管理システム」と「Cisco IoT Field Network Director」は同一製品です。 リリース 3.0 より前では、製品名が「Cisco Connected Grid Network Management System」でした。 現リリース（3.0）では、製品名が「Cisco IoT Field Network Director」（IoT-FND）に変更されています。

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。

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017 年 9 月 6 日

利用規約