Cisco IR800 Integrated Services Router (ISR) モジュール ROMモニタ入力の検証脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170906-isr **初公開日 :** 2017-09-06 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.4 **回避策 :** Yes **Cisco バグ ID :** CSCvb44027	CVE-2017-12223

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 IR800 Integrated Services Router (ISR) モジュール ソフトウェアの ROMモニタ (ROMMON) コードの脆弱性は非認証の、ローカル攻撃者が影響を受けたデバイスの無署名の Hypervisor を起動し、システムの統合を妥協することを可能にする可能性があります。

脆弱性はユーザインプットの不十分な sanitization が原因です。 コンソールによって影響を受けたルータにアクセスできる攻撃者は ROMMON モードを開始することおよび ROMMON 変数を修正する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。 正常なエクスプロイトは攻撃者が任意 の コードを実行し、影響を受けたデバイスで Hypervisor ファームウェアの悪意のあるバージョンをインストール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-20170906-isr

該当製品

修正済みソフトウェア

この脆弱性は Cisco IR800 ソフトウェアに Integrated Services Router (ISR) モジュール影響を与えます。 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。

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-September-06

利用規約