Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア ユーザ名 列挙 情報漏洩の脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170802-asa2 **初公開日 :** 2017-08-02 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.3 **回避策 :** Yes **Cisco バグ ID :** CSCvd47888	CVE-2017-6752

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

の Webインターフェイスの脆弱性はリモート攻撃者 Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）非認証が有効なユーザ名を判別するようにする可能性があります。 攻撃者は追加下検分不正侵入を行なうのにこの情報を使用する可能性があります。

脆弱性はそれらが同時に設定されるとき Lightweight Directory Access Protocol（LDAP）と SSL 接続プロファイル間の相互対話が原因です。 攻撃者はデバイスの IP アドレスにユーザ名 列挙 攻撃の実行によって脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者が有効なユーザ名を判別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があります。

このアドバイザリは、次のリンクより確認できます。
802-asa2

影響を受ける製品

脆弱性が存在する製品

この脆弱性はデバイスが LDAP および SSL 両方接続プロファイルで設定され、パスワード管理が有効に なるとき Cisco ASA 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。

脆弱性が存在しない製品

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。

細部

回避策

ASA 管理者は内蔵パスワード管理をディセーブルにするのに次のコマンドを使用できます:

```
tunnel-group DefaultWEBVPNGroup general-attributes
no password-management
```

固定ソフトウェア

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。

ソース

この脆弱性は Rapid7 の Kirk Hayes によって、バークリー検出されました

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-asa2

改訂履歴

Version	Description	Section	Status	Date
1.0	Initial public release.		Final	2017-August-02

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。