Cisco セキュア ブート ハードウェアの改ざんの脆弱性

High

アドバイザリーID : cisco-sa-20190513-secureboot

初公開日 : 2019-05-13 17:30

最終更新日 : 2019-11-20 17:23

バージョン 1.17 : Final

CVSSスコア : 6.7

回避策 : No workarounds available

Cisco バグ ID : CSCvn77158 CSCvn77159 CSCvn77153 CSCvn77154 CSCvn77155 CSCvn77156 CSCvn77150 CSCvn77151 CSCvn77152 CSCvn89138 CSCvn89137 CSCvn77205 CSCvn77249 CSCvn77207 CSCvn77168 CSCvn77201 CSCvn77245 CSCvn77169 CSCvn77202 CSCvn77246 CSCvn77248 CSCvn77166 CSCvn77167 CSCvn77160 CSCvp42792 CSCvn77162 CSCvn77170 CSCvn89140 CSCvn77209 CSCvn89146 CSCvn89145 CSCvn89144 CSCvn89143 CSCvn77219 CSCvn77212 CSCvn77175 CSCvn77171 CSCvn77172 CSCvn77180 CSCvn77181 CSCvn89150 CSCvn77147 CSCvn77142 CSCvn77143 CSCvn77220 CSCvn77182 CSCvn77183 CSCvn77184 CSCvn77141 CSCvn77185 CSCvn77191

CVE-2019-1649

概要

Cisco 独自のセキュア ブート実装のひとつにおけるアクセス制御ロジックには、ローカルの認証された攻撃者が当該コンポーネントのファームウェアを書き換えることができる脆弱性があります。 この脆弱性はハードウェア ベースのセキュア ブートをサポートする複数のシスコ製品に影響を及ぼします。

この脆弱性はセキュア ブートのハードウェア実装で使用される FPGA (フィールド プログラマブル ゲート アレイ) のオンプレミス アップデートを管理するコードにおける不十分なチェックに起因します。 影響を受ける製品の内部で可動するオペレーティング システムへアクセス可能で、特権を持つ攻撃者が FPGA のファームウェア イメージを書き換えることでこの脆弱性を悪用できます。 脆弱性の不正利用が行われた場合、デバイスは使用不可能となり機器交換が必要になるか、セキュア ブートの確認プロセスが不正に書き換えられ、状況によっては攻撃者が不正なソフトウェア イメージをインストールし、起動させることができるようになる可能性があります。

シスコでは、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する予定です。 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-20190513-secureboot

該当製品

脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示します。

この表には、影響を受ける各製品の Cisco Bug ID が記載されています。 バグの内容には Ciscoバグ 検索ツールよりアクセス可能で、製品特有の追加情報や修正済リリース情報が含まれます。

将来のソフトウェア リリース日が示されている場合、その日付はこのアドバイザリの上部にある最終更新日時点でシスコが把握しているすべての情報に基づいた日付になります。 このソフトウェア リリースの日付は、試験結果や優先される機能や修正の提供等いくつかの理由により変更される場合があります。 影響を受けるコンポーネントについてバージョン情報や日付がリストに記載されていない場合 (空欄や暫定とされているもの)、シスコは修正の評価を続けており、追加情報が確認された時点でアドバイザリを更新します。 アドバイザリが Final とマークされた後、より詳細な情報については関連する Cisco バグを参照して下さい。

Product
Network and Content Security Devices
Cisco ASA 5506-X

Cisco ASA 5506H-X
Cisco ASA 5506W-X
Cisco ASA 5508-X
Cisco ASA 5516-X
Cisco Firepower 2100 シリーズ
Cisco Firepower 4000 シリーズ
Cisco Firepower 9000 シリーズ
Routing and Switching - Enterprise and Service Provider
10/40/100G MR マックスポンダ：暗号化用使用権ライセンス（NCS2K-MR-MXP-LIC）
Cisco NCS 2000 シリーズおよび Cisco ONS 15454 MSTP 用 10 Gbps 光暗号化ライン カード（1545
ASR 903 ルータ、スイッチング プロセッサおよびコントローラ - 400G（A900-RSP3C-400-S）
ASR 907 ルータ、スイッチング プロセッサおよびコントローラ - 400G（A900-RSP3C-400-W）
CBR-8 コンバージド ブロードバンド ルータ
Catalyst 6800 16 ポート 10GE、統合型 DFC4（C6800-16P10G）
Catalyst 6800 32 ポート 10GE、統合型デュアル DFC4（C6800-32P10G）

Catalyst 6800 8 ポート 10GE、統合型 DFC4（C6800-8P10G）
Cisco Catalyst 6800（40 GE ポート X 8、統合型デュアル DFC4-EXL X 2）（C6800-8P40G-XL）
Cisco 1 ポート ギガビット イーサネット WAN ネットワーク インターフェイス モジュール（NIM-1G
Cisco 1120 Connected Grid ルータ
Cisco 1240 Connected Grid ルータ
Cisco 2 ポート ギガビット イーサネット WAN ネットワーク インターフェイス モジュール（NIM-2G
Cisco 3000 シリーズ産業用セキュリティ アプライアンス
Cisco 4000 シリーズ サービス統合型ルータ パケット 1024 チャネル高密度音声 DSP モジュール（S
Cisco 4000 シリーズ サービス統合型ルータ パケット 2048 チャネル高密度音声 DSP モジュール（S
Cisco 4000 シリーズ サービス統合型ルータ パケット 3080 チャネル高密度音声 DSP モジュール（S

Cisco 4000 シリーズ サービス統合型ルータ パケット 768 チャネル高密度音声 DSP モジュール（SM
Cisco 4221 サービス統合型ルータ
Cisco 4321 サービス統合型ルータ
Cisco 4331 サービス統合型ルータ
Cisco 4351 サービス統合型ルータ
Cisco 4431 サービス統合型ルータ
Cisco 4451-X サービス統合型ルータ
Cisco 4461 サービス統合型ルータ
Cisco 5000 シリーズ エンタープライズ ネットワーク コンピュート システム
Cisco 809 Industrial サービス統合型ルータ
Cisco 829 産業用サービス統合型ルータ
Cisco ASR 1000 エンベデッド サービス プロセッサ 200G（ASR1000-ESP200）
Cisco ASR 1000 （6x10GE）（ASR1000-6TGE）
Cisco ASR 1000 固定イーサネット ラインカード, 2x10GE + 20x1GE（ASR1000-2T+20X1GE）
Cisco ASR 1000 シリーズ 100 Gbps エンベデッド サービス プロセッサ（ASR1000-ESP100）
Cisco ASR 1000 シリーズ モジュラ インターフェイス プロセッサ（ASR1000-MIP100）
Cisco ASR 1000 シリーズ ルート プロセッサ 3（Cisco ASR1000-RP3）
Cisco ASR 1001-HX ルータ
Cisco ASR 1001-X
Cisco ASR 1002-HX ルータ
Cisco ASR 900 シリーズ ルート スイッチ プロセッサ（2 ～ 128 G、基本スケール）（A900-RSP2A-
Cisco ASR 900 シリーズ ルート スイッチ プロセッサ（2 ～ 64 G、基本スケール）（A900-RSP2A-6
Cisco ASR 900 シリーズ ルート スイッチ プロセッサ（3 ～ 200 G、大規模スケール）（A900-RSP3
Cisco ASR 9000 シリーズ 16 ポート 100 ギガビット イーサネット ライン カード（A99-16X100GE-X
Cisco ASR 9000 シリーズ 16 ポート 100 ギガビット イーサネット ライン カード（A9K-16X100GE-

Cisco ASR 9000 シリーズ 32 ポート 100 ギガビット イーサネット ラインカード（A99-32X100GE-T
Cisco ASR 9000 シリーズ ルート スイッチ プロセッサ 5（パケット転送用）（A9K-RSP5-TR）
Cisco ASR 9000 シリーズ ルート スイッチ プロセッサ 5（サービス エッジ用）（A9K-RSP5-SE）
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（10 GE および 2 ~ 10 GE、パッシブ冷 4Cu および 4 ~ 10 GE）モジュール型 PSU（ASR-920-20SZ-M）
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（1/10 GE SFP X 12、AC モデル）（AS
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（1/10 GE SFP X 12、DC モデル）（AS
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（12 GE および 2 ~ 10 GE、AC モデル
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（12 GE および 2 ~ 10 GE、DC モデル
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（24 GE 銅線および 4 ~ 10 GE、モジュ
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（24 GE 光ファイバおよび 4 ~ 10 GE、
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（2 GE および 4 ~ 10 GE、AC モデル）
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ 2GE および 4-10GE - DC モデル （ASR
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ （コンフォーマル コーティング：12GE
Cisco ASR 9900 ルート プロセッサ 3（パケット転送用）（A99-RP3-TR）
Cisco ASR 9900 ルート プロセッサ 3（サービス エッジ用）（A99-RP3-SE）
Cisco ASR920 シリーズ - 12GE および 4-10GE、1 IM スロット（ASR-920-12SZ-IM）
Cisco ASR 920 シリーズ - 24GE および 4-10GE - モジュラ PSU および IM（ASR-920-24SZ-IM）
Cisco Catalyst 6800（16 ポート 10 GE、統合型 DFC4-XL）（C6800-16P10G-XL）
Cisco Catalyst 6800（10 GE ポート X 32、統合型デュアル DFC4-XL X 2）（C6800-32P10G-XL）
Cisco Catalyst 6800（8 ポート 10 GE、統合型 DFC4-XL）（C6800-8P10G-XL）
Cisco Catalyst 6800（8 ポート 40 GE、統合型デュアル DFC4-EXL X 2）（C6800-8P40G-XL）
Cisco Catalyst 6800 シリーズ スーパバイザ エンジン 6T（C6800-SUP6T）
Cisco Catalyst 6800 シリーズ スーパバイザ エンジン 6T XL（C6800-SUP6T-XL）
Cisco Catalyst 6816-X シャーシ（標準テーブル）（C6816-X-LE）
Cisco Catalyst 6824-X シャーシおよび 40 G X 2（標準テーブル）（C6824-X-LE-40G）

Cisco Catalyst 6832-X シャーシ（標準テーブル）（C6832-X-LE）
Cisco Catalyst 6840-X シャーシおよび 40G x 2（標準テーブル）（C6840-X-LE-40G）
Cisco Catalyst 9300
Cisco Catalyst 9500 シリーズ高性能スイッチ（1/10/25 G ギガビット イーサネット X 24 + 40/100 G
Cisco Catalyst 9500 シリーズ高性能スイッチ（100 ギガビット イーサネット X 32）（C9500-32C）
Cisco Catalyst 9500 シリーズ高性能スイッチ（40 ギガビット イーサネット X 32）（C9500-32QC）
Cisco Catalyst 9500 シリーズ高性能スイッチ（1/10/25 G ギガビット イーサネット X 48 + 40/100 G
Cisco Catalyst 9500 シリーズ スイッチ（40 G ギガビット イーサネット X 12）（C9500-12Q）
Cisco Catalyst 9500 シリーズ スイッチ（1/10 G ギガビット イーサネット X 16）（C9500-16X）
Cisco Catalyst 9500 シリーズ スイッチ（40 G ギガビット イーサネット X 24）（C9500-24Q）
Cisco Catalyst 9500 シリーズ スイッチ（1/10 G ギガビット イーサネット X 40）（C9500-40X）
Cisco Catalyst 9600 スーパーバイザ エンジン 1
Cisco Catalyst 9800-40 ワイヤレス コントローラ
Cisco Catalyst 9800-80 ワイヤレス コントローラ
Cisco IC3000 産業用コンピューティング ゲートウェイ
Cisco MDS 9000 ファミリ 24/10 SAN 拡張モジュール（DS-X9334-K9）
Cisco NCS 200 シリーズ 10/40/100 G MR マックスポンダ（NCS2K-MR-MXP-K9）
Cisco NCS 5500 12X10、2X40 2XMPA ライン カード ベース（NC55-MOD-A-S）
Cisco NCS 5500 シリーズ 24 ポート 100 GE および 12 ポート 40 GE ハイスケール ライン カード（
Cisco NCS 5500 シリーズ 36 ポート 100 GE ハイスケール ライン カード（NC55-36X100G-A-SE）
Cisco NCS 5504 ファブリック カード（NC55-5504-FC）
Cisco NCS 5516 ファブリック カード（NC55-5516-FC）
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA シャーシ（NCS-55A2-MOD-S）
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA シャーシ（温度耐性強化）（NCS-55A2-MOD-HD
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA シャーシ（温度耐性強化、コンフォーマル コーテ

Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA スケール シャーシ（NCS-55A2-MOD-SE-S）
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA スケール シャーシ（コンフォーマル コーティング
Cisco NCS5501 10G X 40 および 100 G X 4 スケール シャーシ（NCS-5501-SE）
Cisco NCS5501 固定 10G X 48 および 100 G X 6 シャーシ（NCS-5501）
Cisco NCS5502 100 G X 48 スケール シャーシ（NCS-5502-SE）
Cisco NCS5502 固定 100 G X 48 シャーシ（NCS-5502）
Cisco NCS55A1 固定 100 G X 24 シャーシ（NCS-55A1-24H）
Cisco NCS55A1 固定 100 G X 36 ベース シャーシ（NCS-55A1-36H-S）
Cisco NCS55A1 固定 100 G X 36 スケール シャーシ（NCS-55A1-36H-SE-S）
Cisco Network Convergence System 1001
Cisco Network Convergence System 1002
Cisco Network Convergence System 5001
Cisco Network Convergence System 5002
Cisco ネットワーク コンバージェンスシステム 540（N540-ACC-SYS、N540-24Z8Q2C-M、 N540-2
Cisco ネットワーク コンバージェンス システム 540 コンフォーマル コーティング（N540X-ACC-SY
Cisco Network Convergence System 5500 シリーズ 1.2 Tbps IPoDWDM モジュール型ライン カード
Cisco Network Convergence System 5500 シリーズ 36X100G MACsec モジュラ ライン カード（NC
Cisco Nexus 31108PC-V（SFP+ ポート X 48 および QSFP28 ポート X 6）（N3K-C31108PC-V）
Cisco Nexus 31108TC-V（10 G BASE-T RJ-45 ポート X 48 および QSFP28 ポート X 6）（N3K-C31
Cisco Nexus 3132C-Z スイッチ（N3K-C3132C-Z）
Cisco Nexus 3264C-E スイッチ（N3K-C3264C-E）
Cisco Nexus 7000 M3 シリーズ 48 ポート 1/10 G イーサネット モジュール（N7K-M348XP-25L）
Cisco Nexus 7700 F4 シリーズ 30 ポート 100 G イーサネット モジュール（N77-F430CQ-36）

Cisco Nexus 7700 M3 シリーズ 12 ポート 100 G イーサネット モジュール（N77-M312CQ-26L）
Cisco Nexus 7700 M3 シリーズ 24 ポート 40 G イーサネット モジュール（N7K-M324FQ-25L）
Cisco Nexus 7700 M3 シリーズ 48 ポート 1/10 G イーサネット モジュール（N77-M348XP-23L）
Cisco Nexus 7700 スーパーバイザ 3（N77-SUP3E）
Cisco Nexus 9200（40G 100G QSFP28 ポート X 36（N9K-C9236C））
Cisco Nexus 9200（1/10G/25G SFP+ ポート X 48 および 40G QSFP ポート X 6 または 100G QSFP
Cisco Nexus 9200（10/25 Gbps ポート X 48、100G QSFP28 ポート X 18）（N9K-C92300YC）
Cisco Nexus 9200（40G QSFP+ ポート X 56 および 100G QSFP28 ポート X 8（N9K-C92304QC）
Cisco Nexus 9200（40G QSFP+ ポート X 72）（N9K-C9272Q）

Cisco Nexus 9300（1/10G/25G SFP ポート X 48、40G/100G QSFP28 ポート X 6、MACsec、ユニフ
Cisco Nexus 9300（100M/1G BASE-T ポート X 48、10/25G SFP28 ポート X 4、40G/100G SFP28 ポ
Cisco Nexus 9300（10G BASE-T ポート X 48、40G/100G QSFP28 ポート X 6、MACsec 対応）（N
Cisco Nexus 9332C スパイン スイッチ（40/100G QSFP28 ポート X 32、 1/10G SFP ポート X 2（N
Cisco Nexus 9364C スパイン スイッチ（40/100G QSFP28 ポート X 64、 1/10G SFP ポート X 2（N
Cisco Nexus 9500 4 コア/4 スレッド スーパーバイザ（N9K-SUP-A）
Cisco Nexus 9500 6 コア/12 スレッド スーパーバイザ（N9K-SUP-B）
Cisco Nexus 9000 固定、40G/100G QSFP28 ポート X 32（N9K-C9232C））
Cisco Nexus 9000 固定、40G/100G QSFP28 ポート X 36（N9K-C9336C-FX2）
Cisco Nexus 9000 固定（1/10G/25G SFP ポート X 48、40G/100G QSFP28 ポート X 12）（N9K-C9
Cisco Nexus 9000 固定（1/10G/25G SFP ポート X 48、40G/100G QSFP28 ポート X 6）（N9K-C93
Cisco Nexus 9000 固定（10G BASE-T ポート X 48、40G/100G QSFP28 ポート X 6）（N9K-C93108
Cisco Nexus 9000 固定（40/50G QSFP+ ポート X 32（最大）または 100G QSFP28 ポート X 18（最

Cisco Packet-over-T3/E3 サービス モジュール（SM-X-1T3/E3）
Cisco cBR-8 統合型 CCAP 40G リモート PHY ライン カード（CBR-CCAP-LC-40G-R）
MDS 9700 48 ポート 32 Gbps ファイバ チャネル スイッチング モジュール（DS-X9648-1536K9）
Nexus 9500 用スーパーバイザ A+（N9K-SUP-A+）
Nexus 9500 用スーパーバイザ B+（N9K-SUP-B+）
Voice and Unified Communications Devices
Cisco 4000 シリーズ ISR 用アナログ音声ネットワーク インターフェイス モジュール（NIM-2FXO、4FXSP、NIM-2FXS/4FXOP、NIM-4E/M、NIM-2BRI-NT/TE、NIM-4BRI-NT/TE）
Cisco 4000 シリーズ サービス統合型ルータ T1/E1 音声および WAN ネットワーク インターフェイス 8MFT-T1/E1、NIM-1CE1T1-PRI、NIM-2CE1T1-PRI、NIM-8CE1T1-PRI）

脆弱性を含んでいないことが確認された製品

Cisco はすべてのハードウェア ベースのセキュア ブート機能をサポートする製品について、適切なアクセス制御の確認が遵守されているか確認しました。

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

ハードウェア ベースのセキュア ブートをサポートし、脆弱性の影響を受ける Cisco 製品は他にありません。

詳細

この脆弱性を不正利用するためには、攻撃者は以下の全ての条件を満たす必要があります。

- デバイスに対して特権のある管理者権限を持っている
- デバイスの内部で可動するオペレーティング システムにアクセスが可能; これは文書化され、サポートされる方法が用いられる場合と、攻撃者が他の脆弱性を不正利用してアクセスを得る場合があります。
- プラットフォームごとに不正利用手段を開発するか入手できること。 攻撃者が影響を受ける

複数のプラットフォームに対してこの脆弱性を不正利用しようとする場合は、各プラットフォームごとに不正利用の手段を調査する必要があります。 調査手法は異なるプラットフォームに対して再利用できる場合がありますが、あるハードウェア プラットフォーム用に開発された不正利用手法が異なるハードウェア プラットフォームで機能する可能性が高くありません。

すべての影響を受けるプラットフォームについて、Cisco はソフトウェア修正の開発とリリース対応を実行中です。 ほとんどの場合、修正は正常なデバイスのオペレーションに必要となる低レベルのハードウェア コンポーネントをオンプレミスでリプログラムすることが必要になります。 このリプログラミング プロセスで障害が起きると、デバイスが使用不能になり、ハードウェアの交換が必要になることがあります。 以下に関する情報は、それぞれのプラットフォームに対応する Cisco バグのリリース ノートをご参照ください:

1. リプログラム処理の失敗を引き起こす要因やデバイスが使用不可能になる要因
2.
3. ある特定のデバイスが脆弱性の影響を受け、修正が必要なファームウェア バージョンを実行しているか、または既に修正済みバージョンを実行しているかを確認する手順

それぞれのプラットフォーム固有の修正済みソフトウェア リリースに対するリリース ノートには前述のリストの項目 2 および 3 についての詳細な情報が含まれます。 製品のリリース ノートは、これらの項目に関する最新の情報源になります。

セキュア ブートおよび Trustworthy テクノロジーの詳細については、Trustworthy Technologies Datasheet をご参照ください。 セキュア ブート テクノロジーをサポートする全シスコ製品リストは以下をご参照ください。 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-boot-product-list.pdf

回避策

この脆弱性に対処する回避策はありません。

Cisco IOS デバイスの強化ガイドにデバイスを強化して管理アクセスのセキュリティを確保する方法が記載されています。 この文書の推奨事項を設定することで、この脆弱性に対する攻撃ポイントを削減できます。

修正済みソフトウェア

修正済みソフトウェア リリースの詳細については、本アドバイザリの「脆弱性のある製品」セクションに記載されている Cisco Bug ID を参照してください。

シスコでは、このアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供する予定です。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスし

たり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

不正利用事例と公式発表

この脆弱性は Red Balloon Security によって 2019 年 5 月 13 日に公開されました。

Cisco PSIRT（Product Security Incident Response Team）は、この脆弱性を Cisco ASR 1001-X において確認可能な概念実証コードの存在を認識しています。 現時点において、この概念実証コードが一般に入手可能であることを示唆する情報は得ていません。

Cisco PSIRT はこのアドバイザリに説明がある脆弱性の不正利用の発生を認識していません。

出典

Cisco はこの脆弱性を報告し、情報公開に協力いただいた Red Balloon Security の Jatin Kataria

氏（主席研究者）、Richard Housley 氏（研究科学者）、および Ang Cui 博士（チーフサイエンティスト）に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.17	一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	最終版	2019年11月20日
1.16	一部の製品の修正バージョンが更新されました。	脆弱性のある製品	最終版	2019年9月6日
1.15	脆弱性が存在する製品のリストを更新。	脆弱性のある製品	最終版	2019年9月3日
1.14	脆弱性が存在する製品のリストを更新。	脆弱性のある製品	最終版	2019月8月21日
1.13	一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	最終版	2019年8月2日
1.12	一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	最終版	20

				19年7月17日
1.11	一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	最終版	2019年6月28日
1.10	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	最終版	2019年6月17日
1.9	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。 ドキュメントのステータスを最終版に変更。 アドバイザリが更新されることを示した文を削除（概要および脆弱性のある製品）。	概要および脆弱性のある製品	最終版	2019年6月10日
1.8	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	Interim	2019年5月30日
1.7	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品、詳細	Interim	2019年5月23日
1.6	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	Interim	2019年5月22日
1.5	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	Interim	2019年

				5月20日
1.4	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	Interim	2019年5月16日
1.3	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	Interim	2019年5月15日
1.2	脆弱性が存在する製品のリストを更新。 一部の製品向けに修正プログラムの提供日を更新。	脆弱性のある製品	Interim	2019年5月14日
1.1	脆弱性が存在する製品のリストを更新。 Cisco Trustworthy テクノロジーのデータシートのリンクを追加。	脆弱性が存在する製品、詳細	Interim	2019年5月13日
1.0	初回公開リリース		Interim	2019年5月13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。