CPU に対するサイドチャネル攻撃による情報漏えいの脆弱性： 2018 年 5 月

Medium	**アドバイザリーID :** cisco-sa-20180521-cpusidechannel **初公開日 :** 2018-05-22 01:00 **最終更新日 :** 2018-07-06 21:09 **バージョン 1.12 :** Interim **回避策 :** No workarounds available **Cisco バグ ID :**	CVE-2018-3640 CVE-2018-3639

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

2018 年 5月 21 日で、研究者は側チャネル情報の漏えい不正侵入を行う多くの現代マイクロプロセッサ アーキテクチャに関する手順の推測的な実行の実装を利用する 2 脆弱性を表わしました。これらの脆弱性は権限のない、ローカル攻撃者が、特別な場合に他のプロセスに属する特権メモリを読むことを可能にする、可能性があります。

最初の脆弱性は、CVE-2018-3639、*幽霊バリアント 4* か *SpectreNG* として知られています。2つめの脆弱性は、CVE-2018-3640、*幽霊バリアント 3a* として知られています。 両方の不正侵入は表わされたデータを推論するために 2018 年 1 月に表われる不正侵入およびレバレッジ キャッシュ タイミング不正侵入のバリアントです。

これらの脆弱性の不正利用するために、攻撃者は影響を受けたデバイスの巧妙に細工されたかスクリプト コードを実行できる必要があります。 製品やサービスの基盤となる CPU とオペレーティング システムの組み合わせによってはこれらの脆弱性の影響を受ける可能性がありますが、シスコ製品の大半はクローズド システムであり、お客様がデバイス上でカスタム コードを実行することはできないため、脆弱ではありません。 脆弱性を不正利用するための手段は存在しません。シスコ製品は、お客様が、同じマイクロプロセッサ上で、カスタム コードをシスコのコードと並列で実行することを許可している場合にのみ、脆弱になるものと考えられます。

仮想マシンやコンテナとして導入されているシスコ製品においては、これらの脆弱性から直接影響を受けることはありませんが、ホスティング環境が脆弱である場合は、攻撃の対象となる可能性があります。 お客様は、ご利用の仮想環境のセキュリティの強化、ユーザ アクセスの厳密な制御、すべてのセキュリティ アップデートが適用されていることの確認を実施してください。 マルチテナント ホスティング環境で仮想デバイスとして製品を展開しているお客様は、基盤となるハードウェア、およびオペレーティング システムまたはハイパーバイザに、該当の脆弱性に対する

パッチが適用されていることを確認してください。

シスコのクラウド サービスがこれらの脆弱性によって直接影響されることはありませんが、サービスが稼働しているインフラストラクチが影響を受ける可能性はあります。 シスコのクラウド サービスに対するこれらの脆弱性の影響については、このアドバイザリの「該当製品」セクションを参照してください。

シスコでは、これらの脆弱性に対するソフトウェア アップデートを提供する予定です。 これら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-20180521-cpusidechannel

該当製品

シスコでは、これらの脆弱性の影響を受ける製品およびクラウド サービスを判断するために、製品ラインを調査中です。 調査の進捗に応じて、シスコは該当する各製品またはサービスの Cisco Bug ID など、本アドバイザリ内の情報を更新します。

本アドバイザリの「調査中の製品」または「脆弱性が存在する製品」セクションに記載されていない製品またはサービスは、脆弱性が存在しないと判断されています。 製品に脆弱性が存在するかどうかの判断基準は、本アドバイザリの「要約」セクションに記載されています。 この脆弱性については現在調査中のため、現在脆弱性が存在しないと判断されている製品またはサービスが、その後追加の情報が明らかになるにつれて脆弱性が存在すると判断される場合もありますのでご注意ください。

調査中の製品

ネットワーク アプリケーション、サービス、およびアクセラレーション

- Cisco vManage NMS

シスコ クラウド ホステッド サービス

- Cisco Spark
- Cisco Threat Grid

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およびクラウド サービスを示します。

Product	Cisco Bug ID	Fixed Release Availability
Network Application, Service, and Acceleration		
Cisco Wide Area Application Services（WAAS）	CSCvj59144	v6.x へのアップデート（利用可能な）
Cisco vBond Orchestrator		18.2（利用可能）
Cisco vEdge 5000		18.2（利用可能）
Cisco vEdge Cloud		18.2（利用可能）
Cisco vSmart Controller		18.2（利用可能）
Network Management and Provisioning		
シスコ ネットワーク機能仮想化インフラストラクチャ ソフトウェア	CSCvj59161	修正はアップストリーム ベンダーで保留中です
Routing and Switching - Enterprise and Service Provider		
Cisco 4000 シリーズ サービス統合型ルータ（IOS XE オープン サービス コンテナ）	CSCvj59152	修正はアップストリーム ベンダーで保留中です
Cisco 800 シリーズ産業用サービス統合型ルータ	CSCvj59153	修正はアップストリーム ベンダーで保留中です
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ RP2/RP3（IOS XE オープン サービス コンテナ）	CSCvj59152	修正はアップストリーム ベンダーで保留中です
Cisco ASR 1001-HX シリーズ アグリゲーション サービス ルータ（IOS XE オープン サービス コンテナ）	CSCvj59152	修正はアップストリーム ベンダーで保留中です
Cisco ASR 1001-X シリーズ アグリゲーション サービス ルータ（IOS XE オープン サービス コンテナ）	CSCvj59152	修正はアップストリーム ベンダーで保留中です
Cisco ASR 1002-HX シリーズ アグリゲーション サービス ルータ（IOS XE オープン サービス コンテナ）	CSCvj59152	修正はアップストリーム ベンダーで保留中です
Cisco ASR 1002-X シリーズ アグリゲーション サービス ルータ（IOS XE オープン サービス コンテナ）	CSCvj59152	修正はアップストリーム ベンダーで保留中です
Cisco ASR 9000 XR 64 ビット シリーズ ルータ	CSCvj59142	修正はアップストリーム ベンダーで保留中です
Cisco Application Policy Infrastructure Controller（APIC）	CSCvj59131	修正はアップストリーム ベンダーで保留中です
Cisco CGR 1000 コンピューティング モジュール（IOx 搭載）	CSCvj59160	修正はアップストリーム ベンダーで保留中です
Cisco Catalyst 9300 シリーズ スイッチ- IOx 機能	CSCvj59156	修正はアップストリーム ベンダーで保留中です
Cisco Catalyst 9400 シリーズ スイッチ- IOx 機能	CSCvj59157	修正はアップストリーム ベンダーで保留中です
Cisco Catalyst 9500 シリーズ スイッチ- IOx 機能	CSCvj59158	修正はアップストリーム ベンダーで保留中です
Cisco Cloud Services Platform 2100	CSCvj63868	修正はアップストリーム ベンダーで保留中です
シスコ クラウド サービス ルータ 1000V シリーズ（IOS XE オープン サービス コンテナ）	CSCvj59152	修正はアップストリーム ベンダーで保留中です

Cisco NCS 1000 シリーズ ルータ	CSCvj59142	修正はアップストリーム ベンダーで保留中です
Cisco NCS 5000 シリーズ ルータ	CSCvj59142	修正はアップストリーム ベンダーで保留中です
Cisco NCS 5500 シリーズ ルータ	CSCvj59142	修正はアップストリーム ベンダーで保留中です
Cisco Nexus 3000 Series Switches	CSCvj59136	修正はアップストリーム ベンダーで保留中です
Cisco Nexus 5000 シリーズ スイッチ（OAC 機能）	CSCvj59138	
Cisco Nexus 6000 シリーズ スイッチ（OAC 機能）	CSCvj59135	修正はアップストリーム ベンダーで保留中です
Cisco Nexus 7000 シリーズ スイッチ（OAC 機能、Feature Bash）	CSCvj59135	修正はアップストリーム ベンダーで保留中です
Cisco Nexus 9000 シリーズ スイッチ（スタンドアロン、NX-OS モード）	CSCvj59136	修正はアップストリーム ベンダーで保留中です
Cisco Virtual Application Policy Infrastructure Controller（APIC）	CSCvj59131	修正はアップストリーム ベンダーで保留中です
Cisco XRv 9000 シリーズ ルータ	CSCvj59142	修正はアップストリーム ベンダーで保留中です
Unified Computing		
Cisco C880 M4 サーバ	CSCvj59127	修正はアップストリーム ベンダーで保留中です
Cisco C880 M5 サーバ	CSCvj59127	修正はアップストリーム ベンダーで保留中です
シスコ エンタープライズ ネットワーク コンピューティング システム 5100 シリーズ サーバ	CSCvj59121	修正はアップストリーム ベンダーで保留中です
シスコ エンタープライズ ネットワーク コンピューティング システム 5400 シリーズ サーバ	CSCvj59121	修正はアップストリーム ベンダーで保留中です
Cisco HyperFlex with VMWare Hypervisor	CSCvj59134	
Cisco UCS B シリーズ M2 ブレード サーバ-管理される	CSCvj59301	修正はアップストリーム ベンダーで保留中です
Cisco UCS B シリーズ M3 ブレード サーバ	CSCvj54880	Cisco UCS B シリーズ M3 ブレード サーバ（July 2018）推定される
Cisco UCS B シリーズ M4 ブレード サーバ（B260 および B460 を除く）	CSCvj54187	UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS Cシリーズ M4 ラック サーバ-管理される（C460 を除く） - UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS S3260 M4 ストレージ サーバ-管理される- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS S3260 M4 ストレージ サーバ-スタンドアロン- Cisco IMC 3.0(4e) – 6月 25 2018 年
Cisco UCS B シリーズ M5 ブレード サーバ	CSCvj59266	Cisco UCS B シリーズ M5 ブレード サーバ（July 2018）推定される

		Cisco UCS Cシリーズ M5 ラック サーバ（July 2018）推定される
Cisco UCS B260 M4 ブレード サーバ	CSCvj54847	Cisco UCS B260 M4 ブレード サーバ- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS B460 M4 ブレード サーバ- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS C460 M4 ラック サーバ-管理される- UCS Manager 3.2(3e) – 6月 25 2018 年
Cisco UCS B460 M4 ブレード サーバ	CSCvj54847	Cisco UCS B260 M4 ブレード サーバ- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS B460 M4 ブレード サーバ- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS C460 M4 ラック サーバ-管理される- UCS Manager 3.2(3e) – 6月 25 2018 年
Cisco UCS Cシリーズ M2 ラック サーバ-管理される	CSCvj59301	修正はアップストリーム ベンダーで保留中です
Cisco UCS Cシリーズ M2 ラック サーバ-スタンドアロン	CSCvj59309	修正はアップストリーム ベンダーで保留中です
Cisco UCS Cシリーズ M2 ラック サーバ[EX プロセッサ ファミリー サーバ スタンドアロン] -	CSCvj59304	修正はアップストリーム ベンダーで保留中です
Cisco UCS C シリーズ M3 ラック サーバ	CSCvj59312	Cisco UCS Cシリーズ M3 ラック サーバ（July 2018）推定される
Cisco UCS Cシリーズ M4 ラック サーバ（C460 を除く）-スタンドアロン [1]	CSCvj59318	Cisco IMC 3.0(4e) – 6月 25 2018 年
Cisco UCS Cシリーズ M4 ラック サーバ（C460 を除く）-管理された [1]	CSCvj54187	UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS Cシリーズ M4 ラック サーバ-管理される（C460 を除く） - UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS S3260 M4 ストレージ サーバ-管理される- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS S3260 M4 ストレージ サーバ-スタンドアロン- Cisco IMC 3.0(4e) – 6月 25 2018 年
Cisco UCS Cシリーズ M5 ラック サーバ-管理された [1]	CSCvj59331	Cisco UCS Cシリーズ M5 ラック サーバ（July 2018）推定される
Cisco UCS Cシリーズ M5 ラック サーバ-スタンドアロン [1]	CSCvj59266	Cisco UCS B シリーズ M5 ブレード サーバ（July 2018）推定される Cisco UCS Cシリーズ M5 ラック サーバ（July 2018）推定される
Cisco UCS C460 M4 ラック サーバ-管理される	CSCvj54847	Cisco UCS B260 M4 ブレード サーバ- UCS Manager 3.2(3e) – 6月

		25 2018 年 Cisco UCS B460 M4 ブレード サーバ- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS C460 M4 ラック サーバ-管理される- UCS Manager 3.2(3e) – 6月 25 2018 年
Cisco UCS C460 M4 ラック サーバ-スタンドアロン	CSCvj59326	Cisco IMC 3.0(4e) – 6月 25 2018 年
Cisco UCS E シリーズ M2 サーバ	CSCvj59121	修正はアップストリーム ベンダーで保留中です
Cisco UCS E シリーズ M3 サーバ	CSCvj59121	修正はアップストリーム ベンダーで保留中です
Cisco UCS S3260 M4 ストレージ サーバ	CSCvj54187	UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS Cシリーズ M4 ラック サーバ-管理される（C460 を除く） - UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS S3260 M4 ストレージ サーバ-管理される- UCS Manager 3.2(3e) – 6月 25 2018 年 Cisco UCS S3260 M4 ストレージ サーバ-スタンドアロン- Cisco IMC 3.0(4e) – 6月 25 2018 年
Cisco バーチャル インフラストラクチャ マネージャ	CSCvj75271	2.4.1 2.2.24 (Available)
Voice and Unified Communications Devices		
Cisco Remote Expert モバイル	CSCvj59167	修正はアップストリーム ベンダーで保留中です
シスコ クラウド ホステッド サービス		
Cisco Metacloud	CSCvj59149	修正はアップストリーム ベンダーで保留中です

[1] Cisco UCS M4 および M5 ラック サーバは、Cisco HyperFlex ソリューションの一部として使用されています。

脆弱性を含んでいないことが確認された製品

以下のシスコ製品はこれらの製品グループの 4.特定のモデルが影響を受けるかもしれない先行する「脆弱性が存在する製品」セクションに明示的にリストされています幽霊バリアント 3a か幽霊バリアントに脆弱考慮され。

ルータ

ブランチ ルータ

- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco 1900 シリーズ サービス統合型ルータ
- Cisco 1800 シリーズ Integrated Services Router
- Cisco 1000 シリーズ 統合サービス ルータ
- Cisco 800 シリーズ ルータ

データセンター相互接続プラットフォーム

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cisco Carrier Routing System
- Cisco Catalyst 6500 シリーズ スイッチ

産業用ルータ

- Cisco 2000 シリーズ Connected Grid ルータ
- Cisco 1000 シリーズ Connected Grid ルータ
- Cisco 900 シリーズ産業用ルータ
- Cisco 800 シリーズ産業用サービス統合型ルータ
- Cisco 500 シリーズ WPAN 産業用ルータ
- LoRaWAN 向けシスコ ワイヤレス ゲートウェイ

クラウド ネットワーキング サービス

- シスコ クラウド サービス ルータ 1000V シリーズ

モバイル インターネット ルータ

- Cisco 5900 シリーズ エンベデッド サービス ルータ
- Cisco MWR 2900 シリーズ モバイル ワイヤレス ルータ

サービス プロバイダー コア ルータ

- Cisco Carrier Routing System
- Cisco Network Convergence System 6000 シリーズ ルータ

サービス プロバイダー エッジ ルータ

- Cisco 12000 シリーズ ルータ
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cisco ASR 920 シリーズ アグリゲーション サービス ルータ
- Cisco ASR 901 シリーズ アグリゲーション サービス ルータ
- Cisco ASR 900 シリーズ アグリゲーション サービス ルータ
- Cisco XR 12000 シリーズ ルータ
- Ciscoネットワーク コンバージェンス システム 500 シリーズ ルータ

中小規模企業向けルータ

- Cisco 1900 シリーズ サービス統合型ルータ

- Cisco 800 シリーズ ルータ
- Cisco Small Business RV シリーズ ルータ

仮想ルータ

- シスコ クラウド サービス ルータ 1000V シリーズ
- Cisco WAN アグリゲーションとインターネット エッジ ルータ
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cisco Catalyst 6500 シリーズ スイッチ

WAN 最適化

- Cisco Virtual Wide Area Application Services（vWAAS）
- Cisco Wide Area Application Services（WAAS）Express
- Cisco Wide Area Application Services（WAAS）ソフトウェア

スイッチ

ブレード スイッチ

- Cisco Blade Switch Dell 仕様
- Cisco Blade Switch FSC 仕様
- Cisco Blade Switch HP 仕様
- Cisco Nexus 4000 シリーズ スイッチ
- Cisco スイッチ モジュール IBM 仕様
- Cisco ブレード スイッチ用 SFS ソリューション
- Cisco SFS Solution for Dell

キャンパス LAN スイッチ - アクセス

- Cisco Catalyst 9400
- Cisco Catalyst 9300
- Cisco Catalyst 4500 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 3750 シリーズ スイッチ
- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 2960-L シリーズ スイッチ
- Cisco Catalyst 2960-Plus シリーズ スイッチ
- Cisco Catalyst 2960-X シリーズ スイッチ
- Cisco Edge シリーズ
- Cisco Meraki クラウド管理型スイッチ
- Cisco Redundant Power System

キャンパス LAN スイッチ - コアおよびディストリビューション

- Cisco Catalyst 9500
- Cisco Catalyst 6800 シリーズ スイッチ

- Cisco Catalyst 6500 シリーズ スイッチ
- Cisco Catalyst 6500 Virtual Switching System 1440
- Cisco Catalyst 4900 シリーズ スイッチ
- Cisco Catalyst 4500 シリーズ スイッチ
- Cisco Catalyst 4500-X シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Nexus 7000 Series Switches

キャンパスLAN スイッチ-デジタル ビルディング

- Cisco Catalyst 3560-CX シリーズ スイッチ
- Cisco Catalyst 2960-C シリーズ スイッチ
- Cisco Catalyst 2960-CX シリーズ スイッチ
- Cisco Catalyst 2960-L シリーズ スイッチ
- Cisco Catalyst デジタル ビルディング シリーズ スイッチ

データ センター用スイッチ

- Cisco Nexus 2000 シリーズ Fabric Extender
- Cisco R シリーズ ラック
- Cisco RP シリーズ配電ユニット
- Cisco データセンターのネットワーク管理
- Cisco Data Center Network Manager
- Cisco Fabric Manager
- Cisco Cisco IOS ソフトウェア搭載データセンター スイッチ
- Cisco Catalyst 6500 シリーズ スイッチ
- Cisco Catalyst 4900 シリーズ スイッチ
- Cisco エネルギー管理
- Cisco Asset Management Suite
- Cisco Energy Management Suite

産業用イーサネット スイッチ

- Cisco 2500 シリーズ Connected Grid スイッチ
- Cisco エンベデッド サービス 2020 シリーズ スイッチ
- Cisco Industrial Ethernet 5000 シリーズ スイッチ
- Cisco Industrial Ethernet 4010 シリーズ スイッチ
- Cisco Industrial Ethernet 4000 シリーズ スイッチ
- Cisco Industrial Ethernet 3010 シリーズ スイッチ
- Cisco Industrial Ethernet 3000 シリーズ スイッチ
- Cisco Industrial Ethernet 2000 シリーズ スイッチ
- Cisco Industrial Ethernet 2000U シリーズ スイッチ
- Cisco Industrial Ethernet 1000 シリーズ スイッチ

InfiniBand スイッチ

- Cisco SFS 7000 シリーズ InfiniBand サーバ スイッチ
- Cisco SFS 3500 シリーズ マルチファブリック サーバ スイッチ
- Cisco SFS 3000 シリーズ マルチファブリック サーバ スイッチ

LAN スイッチ - スモール ビジネス

- Cisco 550X シリーズ スタッカブル マネージド スイッチ
- Cisco 350 シリーズ マネージド スイッチ
- Cisco 350X シリーズ スタッカブル マネージド スイッチ
- Cisco 250 シリーズ スマート スイッチ
- Cisco 220 シリーズ スマートなスイッチ
- Cisco ESW2 シリーズ拡張スイッチ
- Cisco Small Business 300 シリーズ マネージド スイッチ
- Cisco Small Business 200 シリーズ スマート スイッチ
- Cisco Small Business 110 シリーズ アンマネージド スイッチ
- Cisco Small Business スマート スイッチ
- Cisco Small Business スタッカブル マネージド スイッチ
- Cisco Small Business アンマネージド スイッチ

サービス プロバイダー向けスイッチ – アグリゲーション

- Cisco Catalyst 6500 シリーズ スイッチ
- Cisco Catalyst 4500 シリーズ スイッチ
- Cisco ME 4900 シリーズ イーサネット スイッチ
- Cisco ME 3800X シリーズ キャリア イーサネット スイッチ ルータ

サービス プロバイダー向けスイッチ – イーサネット アクセス

- Cisco Catalyst 3750 Metro シリーズ スイッチ
- Cisco ME 3600X シリーズ イーサネット アクセス スイッチ
- Cisco ME 3400 シリーズ イーサネット アクセス スイッチ
- Cisco ME 3400E シリーズ イーサネット アクセス スイッチ
- Cisco ME 1200 シリーズ キャリア イーサネット アクセス デバイス
- Cisco Small Business ギガビット SP スイッチ

仮想ネットワーキング

- シスコ アプリケーション セントリック インフラストラクチャ バーチャル エッジ
- Cisco Application Virtual Switch
- Cisco Cloud Services Platform 2100
- Cisco Nexus 1000V InterCloud
- KVM 向け Cisco Nexus 1000V スイッチ
- Microsoft Hyper-V 向け Cisco Nexus 1000V スイッチ
- VMware vSphere 向け Cisco Nexus 1000V スイッチ

クラウド ネットワーキング サービス

- Cisco Prime 仮想ネットワーク解析モジュール（vNAM）

- Cisco Virtual Security Gateway
- Cisco Virtual Wide Area Application Services（vWAAS）

WAN スイッチ

- Cisco IGX 8400 シリーズ スイッチ

MGX スイッチ

- Cisco MGX 8900 シリーズ スイッチ
- Cisco MGX 8850 ソフトウェア
- Cisco MGX 8800 シリーズ スイッチ
- Cisco MGX 8250 ソフトウェア
- Cisco MGX 8200 シリーズ エッジ コンセントレータ

Wireless

屋内アクセス ポイント

- Cisco Aironet 1815 シリーズ アクセス ポイント
- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 アクセス ポイント

屋外および産業アクセス ポイント

- Cisco Aironet 1540 シリーズ アクセス ポイント
- Cisco Aironet 1560 シリーズ アクセス ポイント
- Cisco Aironet 1570 シリーズ アクセス ポイント

Wireless LAN Controller

- Cisco 3504 ワイヤレス LAN コントローラ
- Cisco 5520 ワイヤレス LAN コントローラ
- Cisco 8540 ワイヤレス LAN コントローラ
- Cisco Virtual Wireless Controller
- Cisco Meraki Cloud によって管理されるアクセス ポイント

セキュリティ

Cisco は製品をクラウド ホストしました

- 製品およびエンドポイント 保護クライアントの Cisco AMP 系列
- Cisco クラウド セキュリティ
- Cisco Cloudlock
- Cisco Umbrella

E メール セキュリティ

- Cisco コンテンツ セキュリティ管理アプライアンス
- Cisco E メール セキュリティ
- Cisco Email Encryption
- Cisco Email Encryption
- Cisco Registered Envelope Service

ファイアウォール

- Cisco 3000 シリーズ産業用セキュリティ アプライアンス（ISA）（ISA）
- Cisco Meraki クラウド管理型セキュリティ アプライアンス
- Cisco Adaptive Security Appliances（ASA）
- Cisco 適応型セキュリティ仮想アプライアンス（ASAv）（ASAv）

ファイアウォール管理

- Cisco Adaptive Security Device Manager
- Cisco Firepower デバイス マネージャ
- Cisco Firepower Management Center
- Cisco Security Manager

次世代ファイアウォール（NGFW）（NGFW）

- Cisco ASA 5500-X with FirePOWER Services
- Cisco Firepower 9000 シリーズ
- Cisco Firepower 4100 シリーズ
- Cisco Firepower 2100 シリーズ

ネットワーク セキュリティ

- ISR G2 対応 Cisco ワイヤレス コントローラ モジュール

ネットワーク表示およびセグメンテーション

- Cisco ISE パッシブ ID コネクタ
- Cisco Identity Services Engine（ISE）
- Cisco Security Packet Analyzer
- Cisco StealthWatch Cloud
- Cisco StealthWatch エンタープライズ

次世代侵入防御システム（NGIPS）（NGIPS）

- Cisco FirePOWER 8000 シリーズ アプライアンス
- Cisco FirePOWER 7000 シリーズ アプライアンス

セキュリティ管理

- Cisco Firepower Management Center
- Cisco Adaptive Security Device Manager
- Cisco コンテンツ セキュリティ管理アプライアンス
- Cisco Defense Orchestrator

ユニファイド コミュニケーション

- Cisco Spark
- Cisco Unified Communications Manager
- Cisco Business Edition 6000 - 100x80
- Cisco Business Edition 6000
- Cisco Jabber - 100x80
- Cisco Jabber
- Cisco Expressway

カスタマー サポート

- Cisco Unified Contact Center Express
- Cisco Unified Contact Center Enterprise
- Cisco Finesse
- Cisco MediaSense

会議

- Cisco Meeting Server
- Cisco WebEx Meeting Center
- Cisco WebEx Meetings Server
- Cisco TelePresence Management Suite
- Cisco TelePresence Server
- Cisco TelePresence Conductor

コラボレーション エンドポイント

- Cisco 8800 シリーズ IP フォン
- Cisco 7800 シリーズ IP フォン
- Cisco 6900 シリーズ IP フォン
- Cisco 3900 シリーズ SIP 電話
- Cisco Desktop Collaboration Experience DX600 シリーズ
- Cisco DX シリーズ
- Cisco TelePresence SX10 Quick Set
- Cisco TelePresence MX シリーズ- 100x80
- Cisco TelePresence MX Series
- Cisco TelePresence IX5000 シリーズ

Cisco Unified コンピューティング 管理 プラットフォーム

- Cisco Intersight

- Cisco UCS Manager
- Cisco UCS Central
- Cisco UCS Director
- Cisco UCS Performance Manager

IP ビデオ

- Cisco アクセス エッジ
- Ciscoケーブルモデム 終了システム（CMTS）
- Cisco RF スイッチ
- Cisco cBR シリーズ コンバージド ブロードバンド ルータ
- Cisco uBR10000 シリーズ ユニバーサル ブロードバンド ルータ
- Cisco uBR7225VXR ユニバーサル ブロードバンド ルータ
- Cisco uBR7200 シリーズ ユニバーサル ブロードバンド ルータ

他の Cisco IP ビデオプロダクトは影響を受けるために知られていません。

Internet of Things（IoT）

- Cisco 碧玉コントロール センター
- Cisco IoT 管理
- Ciscoアプリケーション Enablement
- Cisco IoT セキュリティ
- 運動 Cisco
- Cisco はエンタープライズを拡張しました

脆弱性が存在しない製品: 追補

以下の製品は「調査中の製品」セクションからこのセクションに移られました:

ネットワーク アプリケーション、サービス、およびアクセラレーション
- Cisco 500 シリーズ WPAN 産業用ルータ（IOx 搭載）
- Cisco DNA センター

ネットワーク管理とプロビジョニング
- Cisco Evolved Programmable Network Manager
- Cisco Meeting Server

ルーティングおよびスイッチング - エンタープライズおよびサービス プロバイダー
- Cisco 1000 シリーズ Connected Grid ルータ
- Cisco Catalyst 3650 シリーズ スイッチ- IOx 機能

- Cisco Industrial Ethernet 4000 シリーズ スイッチ（IOx 搭載）
- Cisco Nexus 4000 Series Blade Switches
- Cisco Nexus 9000 シリーズ ファブリック スイッチ（ACI モード）
- Cisco c800 シリーズ サービス統合型ルータ

ワイヤレス

- LoRaWAN 向けシスコ ワイヤレス ゲートウェイ

シスコ クラウド ホステッド サービス

- Cisco Cloudlock
- Cisco Umbrella
- Cisco WebEx Centers：Meeting Center、Training Center、Event Center、Support Center

詳細

現代 CPU 推測的なストア バイパス情報の漏えい脆弱性

現代のほとんどの CPU の設計における脆弱性により、ローカルの攻撃者がターゲット システム上のセンシティブ情報にアクセスできる可能性があります。

この脆弱性の原因は、投機的実行命令の不適切な実装によるもので、 CPU を現在並べられたメモリの前に読まれる推測的なメモリを行うように試みるために引き起こすことによってこの脆弱性が書きます完了します生じることができます。 攻撃者は任意のコードを実行し、ターゲットのシステムのキャッシュの側チャネル不正侵入を行う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。 不正利用に成功した場合、攻撃者がセンシティブなメモリ情報にアクセスできる可能性があります。

この脆弱性には次の CVE ID が割り当てられています。 CVE-2018-3639

現代 CPU 悪党システム レジスタは情報の漏えい脆弱性を読みました

現代のほとんどの CPU の設計における脆弱性により、ローカルの攻撃者がターゲット システム上のセンシティブ情報にアクセスできる可能性があります。

この脆弱性の原因は、投機的実行命令の不適切な実装によるもので、 この脆弱性は読みますできます影響を受けたプラットフォームを推測的行うために引き起こすことによって誘発されるによってシステム登録の。 攻撃者は任意のコードを実行し、ターゲットのシステムのキャッシュの側チャネル不正侵入を行う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。 不正利用に成功した場合、攻撃者がセンシティブなメモリ情報にアクセスできる可能性があります。

この脆弱性には次の CVE ID が割り当てられています。 CVE-2018-3640

回避策

これら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 リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

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不正利用事例とその公表は確認しておりません。

出典

CVE ID CVE-2018-3639 は Google プロジェクト ゼロ（GPZ）の Jann 角および Microsoft セキュリティ応答センター（MSRC）のケン ジョンソンによって Intel に報告されました。

CVE ID CVE-2018-3640 はズデネック Sojka、ルドルフ Marek、および SYSGO AG からのアレックス Zuepke によって Intel に報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel

改訂履歴

Version	Description	Section	Status	日付
1.12	更新済調査中の製品、脆弱性が存在する製品、および確認された脆弱。	該当製品	Interim	2018-July-06
1.1	脆弱性が存在する製品表にリストされている複数の製品のための修正	該当	Inte	2018-

1	のステータスについての更新された情報。	製品	rim	June-27
1.10	更新済調査中の製品、脆弱性が存在する製品、および確認された脆弱。	該当製品	Interim	2018 年 6 月 22 日
1.9	更新済調査中の製品、脆弱性が存在する製品、および確認された脆弱。	該当製品	Interim	2018-June-13
1.8	該当製品表にリストされている複数の製品のための修正のステータスについての更新された情報。	該当製品	Interim	2018 年 6 月 8 日
1.7	該当製品表にリストされている複数の製品のための修正のステータスについての更新された情報。	該当製品	Interim	2018-June-04
1.6	Affected Products セクション、移動された Cisco 脆弱性が存在する製品 セクションへの 880 の M2 および M3 サーバ。 修正ステータス情報は複数の製品のためにアップデートされました。	該当製品	Interim	2018-June-01
1.5	Affected Products セクションでは、複数の製品は脆弱に調査の下から移動されました。 Cisco DNA センターは調査中に追加されました。	該当製品	Interim	2018-May-31
1.4	Affected Products セクションでは、複数の製品は脆弱に調査の下から移動されました。	該当製品	Interim	2018-May-29
1.3	Affected Products セクションでは、脆弱性が存在しない製品への調査の下から移動された Cisco Evolved Programmable Network Manager。	該当製品	Interim	2018-May-24
1.2	Affected Products セクションでは、複数の製品は脆弱に調査の下から移動されました。	該当製品	Interim	2018-May-23
1.1	Affected Products セクションでは、複数の製品は脆弱 なか確認された脆弱に調査の下から移動されました	該当製品	Interim	2018-May-22
1.0	初回公開リリース		Interim	2018-May-22

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。