

# 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

<b>Medium</b>	アドバイザーID : cisco-sa-20180521-cpusidechannel	<a href="#">CVE-2018-3640</a>
	初公開日 : 2018-05-22 01:00	<a href="#">3640</a>
	最終更新日 : 2018-08-31 20:24	<a href="#">CVE-2018-3639</a>
	バージョン 1.15 : Interim	<a href="#">2018-3639</a>
	回避策 : No workarounds available	
	Cisco バグ ID :	

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、*Spectre variant 4* か *SpectreNG* として知られています。2つめの脆弱性は、CVE-2018-3640、*Spectre Variant 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エーションです。

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カ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。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ャが影響を受ける可能性があります。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

このアドバイザリの「脆弱性が存在する製品」セクションにリストされていない製品がサービスは脆弱考慮されるべきです。製品が脆弱であるかどうか考慮するための基準はこのアドバイザリの「サマリ」セクションで説明されます。

## 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
<b>Network Application, Service, and Acceleration</b>		
Cisco Cloud Services Platform 2100	<a href="#">CSCvj63868</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Wide Area Application Services ( WAAS )	<a href="#">CSCvj59144</a>	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 vManage NMS		
Cisco vSmart Controller		18.2 ( 利用可能 )
<b>Network Management and Provisioning</b>		
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	<a href="#">CSCvj59161</a>	詳細については Cisco バグ ID を参照して下さい
<b>Routing and Switching - Enterprise and Service Provider</b>		
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 )	<a href="#">CSCvj59152</a>	詳細については Cisco バグ ID を参照して下さい
Cisco 800 シリーズ産業用サービス統合型ルータ	<a href="#">CSCvj59153</a>	詳細については Cisco バグ ID を参照して下さい
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	<a href="#">CSCvj59152</a>	詳細については Cisco バグ ID を参照して下さい

サービス コンテナ)		
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 )	<a href="#">CSCvj59152</a>	詳細については Cisco バグ ID を参照して下さい
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 )	<a href="#">CSCvj59152</a>	詳細については Cisco バグ ID を参照して下さい
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 )	<a href="#">CSCvj59152</a>	詳細については Cisco バグ ID を参照して下さい
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 )	<a href="#">CSCvj59152</a>	詳細については Cisco バグ ID を参照して下さい
Cisco ASR 9000 XR 64 ビット シリーズ ルータ	<a href="#">CSCvj59142</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Application Policy Infrastructure Controller ( APIC )	<a href="#">CSCvj59131</a>	詳細については Cisco バグ ID を参照して下さい
Cisco CGR 1000 コンピューティング モジュール ( IOx 搭載 )	<a href="#">CSCvj59160</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Catalyst 9300 シリーズ スイッチ- IOx 機能	<a href="#">CSCvj59156</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Catalyst 9400 シリーズ スイッチ- IOx 機能	<a href="#">CSCvj59157</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Catalyst 9500 シリーズ スイッチ- IOx 機能	<a href="#">CSCvj59158</a>	詳細については Cisco バグ ID を参照して下さい
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 )	<a href="#">CSCvj59152</a>	詳細については Cisco バグ ID を参照して下さい
Cisco NCS 1000 シリーズ ルータ	<a href="#">CSCvj59142</a>	詳細については Cisco バグ ID を参照して下さい
Cisco NCS 5000 シリーズ ルータ	<a href="#">CSCvj59142</a>	詳細については Cisco バグ ID を参照して下さい
Cisco NCS 5500 シリーズ ルータ	<a href="#">CSCvj59142</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Nexus 3000 Series Switches	<a href="#">CSCvj59136</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Nexus 5000 シリーズ スイッチ ( OAC 機能 )	<a href="#">CSCvj59138</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Nexus 6000 シリーズ スイッチ ( OAC 機能 )	<a href="#">CSCvj59135</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Nexus 7000 シリーズ スイッチ ( OAC 機能、 Feature Bash )	<a href="#">CSCvj59135</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Nexus 9000 シリーズ スイッチ ( スタンドアロン、 NX-OS モード )	<a href="#">CSCvj59136</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Virtual Application Policy Infrastructure Controller ( APIC )	<a href="#">CSCvj59131</a>	詳細については Cisco バグ ID を参照して下さい
Cisco XRv 9000 シリーズ ルータ	<a href="#">CSCvj59142</a>	詳細については Cisco バグ ID を参照して下さい
<b>Unified Computing</b>		
Cisco C880 M4 サーバ	<a href="#">CSCvj59127</a>	詳細については Cisco バグ ID を参照して下さい
Cisco C880 M5 サーバ	<a href="#">CSCvj59127</a>	詳細については Cisco バグ ID を参照して下さい

		参照して下さい
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	<a href="#">CSCvj59121</a>	詳細については Cisco バグ ID を参照して下さい
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	<a href="#">CSCvj59121</a>	詳細については Cisco バグ ID を参照して下さい
Cisco HyperFlex with VMWare Hypervisor	<a href="#">CSCvj59134</a>	詳細については Cisco バグ ID を参照して下さい
Cisco UCS B シリーズ M2 ブレード サーバ-管理される	<a href="#">CSCvj59301</a>	Cisco UCS B シリーズ M2 ブレード サーバ-管理される UCS Manager 2.2(8l) - ( 利用可能 ) UCS Manager 3.1(3j) - ( 利用可能 ) UCS Manager 3.2(3g) - ( 利用可能 ) Cisco UCS Cシリーズ M2 ラック サーバ-管理される UCS Manager 2.2(8l) - ( 利用可能 )
Cisco UCS B シリーズ M3 ブレード サーバ	<a href="#">CSCvj54880</a>	UCS Manager 2.2(8l) ( 利用可能な ) UCS Manager 3.1(3j) ( 利用可能な ) UCS Manager 3.2(3g) ( 利用可能な )
Cisco UCS B シリーズ M4 ブレード サーバ ( B260 および B460 を除く )	<a href="#">CSCvj54187</a>	UCS Manager 3.2(3e) - ( 利用可能 ) UCS Manager 3.1(3j) - ( 利用可能 ) UCS Manager 2.2(8l) - ( 利用可能 ) 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) - ( 利用可能 ) Cisco UCS S3260 M4 ストレージ サーバ-管理される- UCS Manager 3.2(3e) - ( 利用可能 ) Cisco UCS S3260 M4 ストレージ サーバ-スタンドアロン- Cisco IMC 3.0(4e) - ( 利用可能 ) Cisco UCS S3260 M4 ストレージ サーバ- UCS Manager 3.1(3j) - ( 利用可能 )
Cisco UCS B シリーズ M5 ブレード サーバ	<a href="#">CSCvj59266</a>	Cisco UCS B シリーズ M5 ブレード サーバ UCS Manager 3.2(3g) - ( 利用可能 ) Cisco UCS Cシリーズ M5 ラック サーバ-スタンドアロン Cisco IMC 3.1(2i) - ( 利用可能 )
Cisco UCS B260 M4 ブレード サーバ	<a href="#">CSCvj54847</a>	Cisco UCS B260 M4 ブレード サーバ

		<p>サーバ  UCS Manager 3.2(3e) - (利用可能)  UCS Manager 3.1(3j) - (利用可能)  UCS Manager 2.2(8l) - (利用可能)  Cisco UCS B460 M4 ブレードサーバ  UCS Manager 3.2(3e) - (利用可能)  UCS Manager 3.1(3j) - 利用可能  UCS Manager 2.2(8l) - 利用可能  Cisco UCS C460 M4 ラックサーバ-管理される  UCS Manager 3.2(3e) - (利用可能)  UCS Manager 3.1(3j) - (利用可能)  UCS Manager 2.2(8l) - (利用可能)</p>
Cisco UCS B460 M4 ブレードサーバ	<a href="#">CSCvj54847</a>	<p>Cisco UCS B260 M4 ブレードサーバ  UCS Manager 3.2(3e) - (利用可能)  UCS Manager 3.1(3j) - (利用可能)  UCS Manager 2.2(8l) - (利用可能)  Cisco UCS B460 M4 ブレードサーバ  UCS Manager 3.2(3e) - (利用可能)  UCS Manager 3.1(3j) - 利用可能  UCS Manager 2.2(8l) - 利用可能  Cisco UCS C460 M4 ラックサーバ-管理される  UCS Manager 3.2(3e) - (利用可能)  UCS Manager 3.1(3j) - (利用可能)  UCS Manager 2.2(8l) - (利用可能)</p>
Cisco UCS Cシリーズ M2 ラックサーバ-管理される	<a href="#">CSCvj59301</a>	<p>Cisco UCS B シリーズ M2 ブレードサーバ-管理される  UCS Manager 2.2(8l) - (利用可能)  UCS Manager 3.1(3j) - (利用可能)  UCS Manager 3.2(3g) - (利用可能)  Cisco UCS Cシリーズ M2 ラックサーバ-管理される</p>

		UCS Manager 2.2(8l) - (利用可能)
Cisco UCS Cシリーズ M2 ラック サーバ-スタンドアロン	<a href="#">CSCvj59309</a>	Cisco IMC 1.4(3z09) - (利用可能)
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]-	<a href="#">CSCvj59304</a>	Cisco IMC 1.5(9f) - (利用可能)
Cisco UCS C シリーズ M3 ラック サーバ	<a href="#">CSCvj59312</a>	UCS Manager 3.2(3g) - (利用可能) UCS Manager 3.1(3j) - (利用可能) UCS Manager 2.2(8l) - (利用可能) Cisco IMC 3.0(4i) - (利用可能) Cisco IMC 2.0(9o) - (利用可能)
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 <sup>1</sup>	<a href="#">CSCvj59318</a>	Cisco IMC 3.0(4e) - (利用可能) Cisco IMC 2.0(10k) - (利用可能)
Cisco UCS Cシリーズ M4 ラック サーバ (C460 を除く) -管理された <sup>1</sup>	<a href="#">CSCvj54187</a>	UCS Manager 3.2(3e) - (利用可能) UCS Manager 3.1(3j) - (利用可能) UCS Manager 2.2(8l) - (利用可能) 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) - (利用可能) Cisco UCS S3260 M4 ストレージサーバ-管理される- UCS Manager 3.2(3e) - (利用可能) Cisco UCS S3260 M4 ストレージサーバ-スタンドアロン- Cisco IMC 3.0(4e) - (利用可能) Cisco UCS S3260 M4 ストレージサーバ- UCS Manager 3.1(3j) - (利用可能)
Cisco UCS Cシリーズ M5 ラック サーバ-管理された <sup>1</sup>	<a href="#">CSCvj59331</a>	UCS Manager 3.2(3g) - (利用可能)
Cisco UCS Cシリーズ M5 ラック サーバ-スタンドアロン <sup>1</sup>	<a href="#">CSCvj59266</a>	Cisco UCS B シリーズ M5 ブレードサーバ UCS Manager 3.2(3g) - (利用可能) Cisco UCS Cシリーズ M5 ラックサーバ-スタンドアロン Cisco IMC 3.1(2i) - (利用可能)
Cisco UCS C460 M4 ラック サーバ-管理される	<a href="#">CSCvj54847</a>	Cisco UCS B260 M4 ブレードサーバ UCS Manager 3.2(3e) - (利用可能) UCS Manager 3.1(3j) - (利用可能) UCS Manager 2.2(8l) - (利用可

		能) Cisco UCS B460 M4 ブレードサーバ UCS Manager 3.2(3e) - (利用可能) UCS Manager 3.1(3j) - 利用可能 UCS Manager 2.2(8l) - 利用可能 Cisco UCS C460 M4 ラックサーバ-管理される UCS Manager 3.2(3e) - (利用可能) UCS Manager 3.1(3j) - (利用可能) UCS Manager 2.2(8l) - (利用可能)
Cisco UCS C460 M4 ラックサーバ-スタンダアロン	<a href="#">CSCvj59326</a>	Cisco IMC 3.0(4e) - (利用可能) Cisco IMC 2.0(12h) - (利用可能)
Cisco UCS E シリーズ M2 サーバ	<a href="#">CSCvj59121</a>	詳細については Cisco バグ ID を参照して下さい
Cisco UCS E シリーズ M3 サーバ	<a href="#">CSCvj59121</a>	詳細については Cisco バグ ID を参照して下さい
Cisco UCS S3260 M4 ストレージサーバ	<a href="#">CSCvj54187</a>	UCS Manager 3.2(3e) - (利用可能) UCS Manager 3.1(3j) - (利用可能) UCS Manager 2.2(8l) - (利用可能) 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) - (利用可能) Cisco UCS S3260 M4 ストレージサーバ-管理される- UCS Manager 3.2(3e) - (利用可能) Cisco UCS S3260 M4 ストレージサーバ-スタンダアロン- Cisco IMC 3.0(4e) - (利用可能) Cisco UCS S3260 M4 ストレージサーバ- UCS Manager 3.1(3j) - (利用可能)
Cisco 仮想な インフラストラクチャ マネージャ	<a href="#">CSCvj75271</a>	2.4.1 2.2.24 (Available)
<b>Voice and Unified Communications Devices</b>		
Cisco Remote Expert モバイル	<a href="#">CSCvj59167</a>	詳細については Cisco バグ ID を参照して下さい
<b>シスコクラウドホステッドサービス</b>		
Cisco Metacloud	<a href="#">CSCvj59149</a>	詳細については Cisco バグ ID を参照して下さい
Cisco Threat Grid		

<sup>1</sup> 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 Spectre Variant 3a もしくは Spectre Variant 4の脆弱性の影響を受けないことが確認されています。これらのプロダクト ファミリーの特定のモデルが脆弱性の影響を受ける場合は、前の「脆弱性のある製品」セクションに明示的に記載されます。

## 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 スタックابل 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 スタックابل 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 スタックابل 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 管理されたアクセス 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*

- Cisco AMP ファミリー製品およびエンドポイント 保護 クライアント
- 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 ( ASA v ) ( ASA v )

*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

*ネットワーク可視性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

**考慮される調査の後で脆弱 ではない 製品**

Cisco は以下の製品を検討し、彼らはこのアドバイザリに説明がある脆弱性から影響を受けると考慮されません:

#### 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 Center

#### ネットワークおよびコンテンツ セキュリティ デバイス

- Cisco Umbrella 仮想アプライアンス

#### 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
- 政府のための Cisco Hosted Collaboration Solution ( HCS )
- Cisco Spark
- 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 情報漏洩の脆弱性

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、この脆弱性は 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書きます完了します引き起こすことができます。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ンネル攻撃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 レジスタは情報漏洩の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せん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引き起こされること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ンネル攻撃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
1.15	UCS M2 ラック サーバのための更新済修正済みソフトウェア 情報; 確認された脆弱 ではない セクションへの政府のための追加された Cisco Hosted Collaboration ソリューション	考慮される調査の後で脆弱 ではない 該当製品 および製品	Interim	2018-August-31
1.14	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のステータスについての更新された情報。 進行中の調査への取除かれた参照。	考慮される調査の後で脆弱 ではない 該当製品 および製品	Interim	2018-August-07
1.13	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-26
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
1.11	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-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	該当製品	Interim	2018-May-31

	調査中に追加されました。			
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

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。