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

Medium	**アドバイザリーID :** cisco-sa-20180104-cpusidechannel **初公開日 :** 2018-01-04 22:20 **最終更新日 :** 2018-02-07 22:16 **バージョン 1.19 :** Interim **回避策 :** No workarounds available **Cisco バグ ID :**	CVE-2017-5753 CVE-2017-5754 CVE-2017-5715

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 1 月 3 日、複数の研究者が 3 つの脆弱性を公表しました。近年の多くのマイクロプロセッサ アーキテクチャに導入されている命令の投機的実行を不正利用し、サイドチャネル攻撃による情報漏えいを行うものです。 これらの脆弱性により、特定の条件下において、権限のないローカル攻撃者が、他のプロセスに属する、権限がなければ読み込めないはずのメモリや、オペレーティング システムのカーネルに割り当てられたメモリを読み取れる可能性があります。

CVE-2017-5753 と CVE-2017-5715 の 2 つの脆弱性は、まとめて *Spectre* と称されており、 3 つ目の CVE-2017-5754 の脆弱性は、 *Meltdown* と呼ばれています。 これらの脆弱性は、投機的実行の不正利用方法が異なりますが、すべて同じ攻撃の亜種です。

攻撃者がこれらの脆弱性を不正利用するには、該当するデバイス上で細工された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。 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-20180104-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

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 Availab
Network Application, Service, and Acceleration		
Cisco Cloud Services Platform 2100	CSCvh32644	アップストリーム サイヤ パッチ保留中
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	CSCvh49919	アップストリーム サイヤ パッチ保留中
Cisco Wide Area Application Services（WAAS）	CSCvh49646	V6.x に更新（すでに ）

Cisco vBond Orchestrator		アップストリーム サイヤ パッチ保留中
Cisco vEdge 5000		アップストリーム サイヤ パッチ保留中
Cisco vEdge Cloud		アップストリーム サイヤ パッチ保留中
Cisco vManage NMS		アップストリーム サイヤ パッチ保留中
Cisco vSmart Controller		アップストリーム サイヤ パッチ保留中
Network Management and Provisioning		
Cisco Application Policy Infrastructure Controller (APIC)	CSCvh58549	アップストリーム サイヤ パッチ保留中
Cisco Evolved Programmable Network Manager	CSCvh64005	アップストリーム サイヤ パッチ保留中
Cisco Virtual Application Policy Infrastructure Controller (APIC)	CSCvh58549	アップストリーム サイヤ パッチ保留中
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)	CSCvh32416	アップストリーム サイヤ パッチ保留中
Cisco 800 （IOx 機能）	CSCvh31418	アップストリーム サイヤ パッチ保留中
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)	CSCvh32416	アップストリーム サイヤ パッチ保留中
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)	CSCvh32416	アップストリーム サイヤ パッチ保留中
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)	CSCvh32416	アップストリーム サイヤ パッチ保留中
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)	CSCvh32416	アップストリーム サイヤ パッチ保留中
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)	CSCvh32416	アップストリーム サイヤ パッチ保留中
Cisco ASR 9000 XR 64 ビット シリーズ ルータ	CSCvh32429	アップストリーム サイヤ パッチ保留中
Cisco CGR 1000 コンピューティング モジュール (IOx 搭載)	CSCvh32516	アップストリーム サイヤ パッチ保留中
Cisco Catalyst 9300 シリーズ スイッチ (オープン サービス コンテナまたは IOx 機能)	CSCvh44164	アップストリーム サイヤ パッチ保留中
Cisco Catalyst 9400 シリーズ スイッチ (オープン サービス コンテナまたは IOx 機能)	CSCvh44165	アップストリーム サイヤ パッチ保留中
Cisco Catalyst 9500 シリーズ スイッチ (オープン サービス コンテナまたは IOx 機能)	CSCvh44166	アップストリーム サイヤ パッチ保留中
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)	CSCvh32416	アップストリーム サイヤ パッチ保留中
Cisco NCS 1000 シリーズ ルータ	CSCvh32429	アップストリーム サイヤ パッチ保留中
Cisco NCS 5000 シリーズ ルータ	CSCvh32429	アップストリーム サイヤ パッチ保留中
Cisco NCS 5500 シリーズ ルータ	CSCvh32429	アップストリーム サイヤ パッチ保留中
Cisco Nexus 3000 Series Switches	CSCvh32392	アップストリーム サイヤ パッチ保留中
Cisco Nexus 3500 Series Switches	CSCvh32393	アップストリーム サ

		イヤ パッチ保留中
Cisco Nexus 5000 シリーズ スイッチ (OAC 機能)	CSCvh32394	アップストリーム サ イヤ パッチ保留中
Cisco Nexus 6000 シリーズ スイッチ (OAC 機能)	CSCvh32390	アップストリーム サ イヤ パッチ保留中
Cisco Nexus 7000 シリーズ スイッチ (OAC 機能、Feature Bash)	CSCvh32390	アップストリーム サ イヤ パッチ保留中
Cisco Nexus 9000 シリーズ スイッチ (スタンドアロン、NX-OS モード)	CSCvh32392	アップストリーム サ イヤ パッチ保留中
Cisco XRv 9000 シリーズ ルータ	CSCvh32429	アップストリーム サ イヤ パッチ保留中
Cisco c800 シリーズ サービス統合型ルータ (IOx 機能)	CSCvh51582	アップストリーム サ イヤ パッチ保留中
Unified Computing		
Cisco C880 M4 サーバ	CSCvh66783	アップストリーム サ イヤ パッチ保留中
Cisco C880 M5 サーバ	CSCvh66783	アップストリーム サ イヤ パッチ保留中
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	CSCvh48274	ETA を修正 (16-Mar 2018)
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	CSCvh48274	ETA を修正 (16-Mar 2018)
Cisco HyperFlex with VMWare Hypervisor	CSCvh68612	アップストリーム サ イヤ パッチ保留中
Cisco UCS B シリーズ M2 ブレード サーバ	CSCvh31576	アップストリーム サ イヤ パッチ保留中
Cisco UCS B シリーズ M3 ブレード サーバ	CSCvg97965	ETA を修正 (16-Mar 2018)
Cisco UCS B シリーズ M4 ブレード サーバ (B260 および B460 を除く)	CSCvg97979	ETA を修正 (16-Mar 2018)
Cisco UCS B シリーズ M5 ブレード サーバ	CSCvh31577	ETA を修正 (16-Mar 2018)
Cisco UCS B260 M4 ブレード サーバ	CSCvg98015	ETA を修正 (16-Mar 2018)
Cisco UCS B460 M4 ブレード サーバ	CSCvg98015	ETA を修正 (16-Mar 2018)
Cisco UCS C シリーズ M2 ラック サーバ	CSCvh31576	アップストリーム サ イヤ パッチ保留中
Cisco UCS C シリーズ M3 ラック サーバ	CSCvg97965	ETA を修正 (16-Mar 2018)
Cisco UCS C シリーズ M4 ラック サーバ (C460 を除く) [1]	CSCvg97979	ETA を修正 (16-Mar 2018)
Cisco UCS C シリーズ M5 ラック サーバ [1]	CSCvh31577	ETA を修正 (16-Mar 2018)
Cisco UCS C460 M4 ラック サーバ	CSCvg98015	ETA を修正 (16-Mar 2018)
Cisco UCS E シリーズ M2 サーバ	CSCvh48274	アップストリーム サ イヤ パッチ保留中
Cisco UCS E シリーズ M3 サーバ	CSCvh48274	アップストリーム サ イヤ パッチ保留中
Cisco UCS M シリーズ モジュラ サーバ	CSCvh55760	修正予定なし
Cisco UCS S3260 M4 ストレージ サーバ	CSCvg97979	ETA を修正 (16-Mar 2018)

Voice and Unified Communications Devices		
Cisco Remote Expert モバイル	CSCvh58132	アップストリーム サイヤ パッチ保留中
Wireless		
LoRaWAN 向けシスコ ワイヤレス ゲートウェイ	CSCvh58504	アップストリーム サイヤ パッチ保留中
シスコ クラウド ホステッド サービス		
Cisco Metacloud Cisco Threat Grid	CSCvh53992	（2018 年 3 月 2 日） （2018 年 2 月 28 日

[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

他のシスコ製品およびクラウド サービスにおいてこれらの脆弱性の影響を受けるものは、現在確認されていません。

シスコは、これらの脆弱性が以下の製品およびクラウド サービスには影響を与えないことを確認しました。

Collaboration and Social Media

- Cisco Meeting Server

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 vEdge 1000
- Cisco vEdge 100
- Cisco vEdge 2000

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 500 シリーズ WPAN 産業用ルータ（IOx 搭載）
- Cisco ASR 1001 固定構成アグリゲーション サービス ルータ
- Cisco ASR 1002 固定構成アグリゲーション サービス ルータ
- Cisco ASR 1002-F 固定構成アグリゲーション サービス ルータ
- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- 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）

シスコ クラウド ホステッド サービス

- Cisco Cloudlock
- シスコ マネージド サービス
- Cisco Meraki
- Cisco Spark
- Cisco Umbrella
- Cisco WebEx Centers：Meeting Center、Training Center、Event Center、Support Center

詳細

これらの脆弱性の詳細については、次のとおりです。

現代の CPU におけるプロセス予測情報漏えいの脆弱性

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。

分岐ターゲット インジェクションによってトリガーされます。 攻撃者は、標的となるシステム上で任意のコードを実行し、サイドチャネル攻撃を行うことで、この脆弱性を不正利用できます。 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-2017-5715

現代の CPU におけるプロセス分岐予測情報漏えいの脆弱性

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。

範囲チェックが回避されることでトリガーされます。 攻撃者は、標的となるシステム上で任意のコードを実行し、サイドチャネル攻撃を行うことで、この脆弱性を不正利用できます。 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-2017-5753

Intel CPU Indirect Branch Prediction Information Disclosure Vulnerability

Intel 製 CPU を搭載したハードウェアの脆弱性により、ローカルの攻撃者が、標的とされる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。

この脆弱性は、サイドチャネル攻撃によるもので、Meltdown 攻撃とも呼ばれます。 攻撃者は、該当のシステム上で任意のコードを実行することで、この脆弱性を不正利用できます。 不正利用

に成功した場合、攻撃者が標的となるシステム上の CPU キャッシュ メモリなど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。

この脆弱性には次の CVE ID が割り当てられています。 CVE-2017-5754

回避策

Cisco bugs 、Cisco Bug Search Tool

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。

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

本アドバイザリに記載されている脆弱性は、2018 年 1 月 3 日の時点で、複数の記事やディスカッション フォーラムに取り上げられています。

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を確認していません。

出典

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180104-cpusidechannel

改訂履歴

Version	Description	Section	Status	日付

1.19	E シリーズ サーバに関する脆弱性が存在する製品の表を更新。	脆弱性のある製品	Interim	2018-February-07
1.18	脆弱性が存在する製品の表の多くの製品について修正リリース/スケジュールを更新。	脆弱性のある製品	Interim	2018-February-07
1.17	脆弱性が存在する製品の表を更新。	脆弱性のある製品	Interim	2018-February-05
1.16	「脆弱性のある製品」と「脆弱性を含んでいないことが確認された製品」のセクションを更新。 Cisco Industrial Ethernet 4000 デバイスを、「脆弱性を含んでいないことが確認された製品」のセクションに移動。	「脆弱性のある製品」、「脆弱性を含んでいないことが確認された製品」	Interim	2018 年 1 月 30 日
1.15	「脆弱性のある製品」のセクションを更新。	脆弱性のある製品	Interim	2018-January-26
1.14	「調査中の製品および脆弱性のある製品」のセクションを更新。	「該当製品」、「脆弱性のある製品」	Interim	2018-January-24
1.13	「調査中の製品および脆弱性のある製品」のセクションを更新。 UCS M5 サーバのファームウェア リリースの日付を削除。この時点で、UCS M5 の BIOS 更新については、cisco.com から削除されています。デバイスの更新については、これらの更新プログラムの次のリビジョンが出るまでお待ちください。	「該当製品」、「脆弱性のある製品」	Interim	2018-January-22
1.12	調査中の製品および脆弱性のある製品に関して更新。	「該当製品」、「脆弱性のある製品」	Interim	2018 年 1 月 19 日
1.	仮想環境内の基盤となるオペレーティング	サマリー、影響を受ける製品、脆弱性	I	2018

1.11	システムおよびハイパーバイザの更新に関するガイダンスを提供するよう、概要セクションを更新。 該当製品セクションおよび修正済みリリースの表を更新。	のある製品	nterim	年 1 月 18 日
1.10	修正済みリリースの提供および予測に関して、脆弱性が存在する製品セクションを更新。	脆弱性のある製品	Interim	2018 年 1 月 17 日
1.9	修正済みリリースの提供を含む、調査中の製品および脆弱性のある製品に関する情報を更新。	該当製品および脆弱性のある製品	Interim	2018 年 1 月 16 日
1.8	修正済みリリースの提供を含む、調査中の製品および脆弱性のある製品に関する情報を更新。	該当製品および脆弱性のある製品	Interim	2018 年 1 月 15 日
1.7	「脆弱性のある製品」、「調査中の製品」、「脆弱性を含んでいないことが確認された製品」に関する情報を更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2018 年 1 月 12 日
1.6	「脆弱性のある製品」、「調査中の製品」、「脆弱性を含んでいないことが確認された製品」に関する情報を更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2018 年 1 月 11 日
1.5	シスコ クラウド サービスのステータスを示すように要約を更新し、管理者にユーザアクセス制御を推奨。「脆弱性のある製品」、「調査中の製品」、「脆弱性を含んでいないことが確認された製品」に関する情報を更新。	「要約」、「該当製品」、「脆弱性が存在する製品」、「脆弱性が存在しないことが確認された製品」	Interim	2018 年 1 月 10 日
1.4	「調査中の製品」および「脆弱性のある製品」の情報を更新。	「該当製品」、「脆弱性のある製品」	Interim	2018 年 1 月 9 日
1.3	「調査中の製品」および「脆弱性を含んでいないことが確認された製品」に関する脆弱性の詳細と情報を更新。「脆弱性のある製品」の表を追加。修正済みリリースの入	「該当製品」「脆弱性のある製品」「詳細」「修正済みソフトウェア」	Inte	2018 年 1 月 8 日

	手状況に関する情報を含む。		rim	
1.2	「概要」と「調査中の製品」を更新。修正情報を含む「脆弱性のある製品」の表を追加。	概要、影響を受ける製品、脆弱性が存在する製品、修正済みソフトウェア。	Interim	2018年1月5日
1.1	脆弱性を含んでいないことが確認された製品セクションを明示しました。	脆弱性を含んでいないことが確認された製品	Interim	2018-January-04
1.0	初回公開リリース		Interim	2018-January-04

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。