— AUS（アルテミス・ユーザ・サポート）便り 2018/01/09号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Intel, AMD, ARM等各社CPUに脆弱性…機密情報読み取りの恐れ

https://news.mynavi.jp/article/20180104-567288/
http://www.itmedia.co.jp/news/articles/1801/04/news009.html
http://www.itmedia.co.jp/news/articles/1801/04/news010.html

このニュースをザックリ言うと･･･

- 1月初頭、Intel社のCPUに機密情報を読み取られる複数の脆弱性が存在すると一部ネットメディアで報じられ、同3日（現地時間）にはIntel社より、同社製品特有ではなく、AMD社やARM社のCPUにも同様の脆弱性が存在するとの声明が出されています。

- 「Meltdown」「Spectre」等と名付けられた脆弱性は、Googleのセキュリティチームやオーストリアのグラーツ工科大学等により、数か月前に確認されたもので、メモリ上に保存されている機密情報がPCやデバイス上の権限のないプログラムから読み取られる恐れがあるとされています（なお、データの改ざん・削除等はできない模様です）。

- 影響はクライアント・サーバPCからスマートデバイス、IoT機器までに及ぶとされ、今回の発表を受け、Windowsについては5日（日本時間）付けで緊急パッチがリリースされた他、各OSやファームウェアでも対応が進んでいます。

AUS便りからの所感等

- 脆弱性を突いた攻撃としては、不正なプログラムがPC等にインストールされて実行されるケースが考えられ、Webページに埋め込まれた不正なスクリプト等からターゲットとなるPC上の情報を直接読み取られるなどの可能性は現時点で低いとみられ、今後アンチウイルスやUTM等で検知できるかは未知数ですが、可能な限り脆弱性の影響を受けないためにも、不審なアプリをインストール・実行しないことを心がけるべきです。

- 一台のハードウェア上で複数の仮想サーバが動作するクラウド等の環境では、特に他のユーザのデータが読み取られるリスクへの懸念があり、Microsoft Azure等のクラウドサービスでは仮想サーバの再起動等を伴うメンテナンスを実施している所もあり、利用しているサービスのメンテナンス情報の確認も行っておきましょう。

- Windowsの緊急セキュリティパッチについては、一部アンチウイルスソフトと干渉する不具合があるとされており、社内への展開等にあたっては、これが解決するまでの間、事前の十分な検証を行うことも検討すべきでしょう（なお、Firefox等のブラウザにおいてもセキュリティアップデートがリリースされており、多重防御の意味でもアップデートを推奨致します）。


マイナビニュース

2018/01/04 11:57:43

Intel、AMD、ARMなどのCPUに深刻な脆弱性、影響を巡る報道で混乱広がる

Yoichi Yamashita

Intel、AMD、ARMなどのモダンCPUの投機的実行（speculative execution）プロセスに深刻な脆弱性が存在することが明らかになった。悪用されると、パスワードや暗号カギといった機密データも記録されるシステムメモリーのデータを第三者に読み取られる可能性がある。

Intel CPUだけの問題に非ず

この脆弱性は「Meltdown」と「Spectre Attacks: Exploiting Speculative Execution」という投機的実行の脆弱性を攻撃する手法に関する論文を紹介する報道で広く知られることになった。報道では当初「IntelのCPUに脆弱性」と報じられたが、1月3日（現地時間）にIntelが「Intel responds to security research findings」という声明を公開し、脆弱性をIntel製品のバグとした報道の誤りを指摘した。脆弱性は投機的実行を採用するモダンCPUの問題であり、AMDやARMなどのプロセッサも影響を受ける。論文を公表した研究者によると、MeltdownがARMやAMDのプロセッサに影響するかは3日時点で「不明」、SpectreはIntel、AMD、ARMのプロセッサで実行できることを確認している。


Intel、プロセッサ脆弱性はAMDやArmにもあり、対策で協力中と説明

2018年01月04日 08時45分 公開　[佐藤由紀子，ITmedia]

印刷　通知　903　227　B!93　142

米Intelは1月3日（現地時間）、複数のセキュリティ研究者が開示したプロセッサの2つの脆弱性について、この問題はIntelのプロセッサ固有のものではなく、米AMDや英Arm、OS提供企業などと対策のために協力していると説明した。

この脆弱性は、オーストリアのグラーツ工科大学や米Googleの研究者が発見し、「Meltdown」と「Spectre」と名付けた。まだ対策はないが、Intelは「現在のメディアによる不正確な報道に対処するため」、脆弱性の存在を認める声明を出したとしている。具体的な対策については「対策のためのソフトウェアおよびファームウェアのアップデートが可能になる来週発表する」という。

Intelによると、この脆弱性を悪用されるとデータを盗まれる可能性はあるが、データを改ざんされたり削除されたりすることはないという。

ユーザーがこの脆弱性に対処するためには、各社のプロセッサを搭載する端末のメーカーやOSメーカーによるソフトウェア／ファームウェアの更新を適用する必要がある。

米Googleは同日、同社製品でユーザーによる何らかの対処を必要とするケースについて説明した。Android端末は、最新セキュリティパッチを適用すれば安全という。Googleアプリ、Google App Engineも影響を受けない。ChromeおよびChrome OSについては、「サイト分離」を有効にすると安全としている。すべての製品についての関連情報はサポートページにまとまっている。


プロセッサ脆弱性「Meltdown」と「Spectre」のまとめサイト開設

2018年01月04日 10時25分 公開　[佐藤由紀子，ITmedia]

印刷　通知　477　226　B!60　135

米Intelが発表したプロセッサの重大な脆弱性についてのまとめサイトが開設された。複数のセキュリティ研究者が発見した2つの脆弱性「Meltdown」と「Spectre」について、基本的な説明があり、技術的な情報および影響を受けるサービスや製品を提供する企業の公式サイトへのリンクなどが掲載されている。

このサイトは2つの脆弱性を発見した組織の1つであるオーストリアのグラーツ工科大学が開設した。Meltdown（崩壊）という名称は、この脆弱性が正常であればハードウェアによって守られるはずのセキュリティ境界を崩壊させることから付けられたという。Spectre（幽霊）は、speculative execution（投機的実行：コンピュータに必要としないかもしれない仕事をさせること）から来ているが、修正が難しく、長く悩まされる可能性があることも示しているという。

MeltdownとSpectreのロゴ

●Mirai亜種がロジテック社等のルータに感染しボットネットを拡大

https://www.jpcert.or.jp/at/2017/at170049.html
http://www.logitec.co.jp/info/2017/1219.html

このニュースをザックリ言うと・・・

- 12月19日（日本時間）、JPCERT/CCより、マルウェア「Mirai」の亜種によるとみられる感染活動が11月から確認されているとして警告が出されています。

- 発表では、マルウェアはロジテック社製のルータの一部に存在する脆弱性を突いて感染を広げているとしており、この他、ファーウェイ社製の日本では発売していない機種のルータに関しても同様の感染活動が確認されています。

- 同日にはロジテック社からも警告が出され、ファームウェアのアップデートを行うよう呼び掛けられています。

AUS便りからの所感等

- 脆弱性はUPnP（ユニバーサル・プラグアンドプレイ）機能に関するものとされ、これを対策するファームウェアは既に2013~2014年にかけてリリースされていたものですが、3年以上前に修正された脆弱性の悪用が成功し、マルウェアの感染拡大の一助となっているということは、こういったルータ等ネットワーク機器へのメンテナンスが十分に行き届いていないことを如実に示していると言えるでしょう。

- PCやスマートデバイス以外のルータ・UTM等各種ネットワーク機器やIoTデバイスについても存在を把握し、ベンダー情報の確認を行い、ファームウェア等のアップデートを確実に行う体制を整えることが肝要です。


JPCERT CC
Mirai 亜種の感染活動に関する注意喚起

各位

JPCERT-AT-2017-0049
JPCERT/CC
2017-12-19

<<< JPCERT/CC Alert 2017-12-19 >>>

Mirai 亜種の感染活動に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170049.html

I. 概要

Logitec

2017/12/19
ロジテック株式会社

ロジテック製300Mbps無線LANブロードバンドルータ
およびセットモデル（全11モデル）に関する重要なお知らせとお願い

お客様各位

平素は格別のご高配を賜り、厚く御礼申し上げます。
ロジテック製 300Mbps無線LANブロードバンドルータおよび、セットモデル（全11モデル）の一部のファームウェアバージョンにおいて、UPnPのセキュリティ脆弱性が確認されました。対象製品をお持ちのお客様におかれましては、最新版のファームウェアに更新されているか、下記の手順にてご確認いただき、アップデートをいただきますようお願い申し上げます。

●日産カナダファイナンス、113万人の顧客データ漏洩の可能性

https://news.mynavi.jp/article/20171226-562662/

このニュースをザックリ言うと・・・

- 12月21日（現地時間）、日産グループのカナダ法人である日産カナダファイナンス（NCF）社より、同社顧客の個人情報が不正アクセスを受け、流出した可能性があると発表されました。

- 被害を受けた可能性があるのは、同社およびINFINITI Financial Services Canadaのローンを利用した顧客113万人分の氏名・住所・車種・車両識別番号・クレジット信用情報およびローンの金額と月々の支払額などとされており、決済カード情報およびカナダ以外の国でローンを利用した顧客の情報については被害はなかったとのことです。

- 同社では12月11日に不正アクセスの痕跡を確認、対象となる顧客に連絡を取り、個人信用情報機関の米TransUnion社による与信監視サービスを12ヶ月間無償提供する他、カナダのプライバシー規制当局や捜査当局に通報、データセキュリティ専門業者と連携しての調査等を行っているとのことです。

AUS便りからの所感等

- 現時点で不正アクセスの経路等の詳細は明らかになっておらず、「標的型攻撃」や「リスト型攻撃」による関係者アカウントの乗っ取り等の可能性が考えられるものの、あくまで推測の域を出ません。

- よってこの段階で言えることは、この機会にこれまでに発生した様々な個人情報流出事件を振り返り、前述した二通りの攻撃をはじめ、主に発生する原因に対する対策の検討、そしてUTM等による防御について十分に行われているかを随時見直しを行うべきである、といったところとなるでしょう。


マイナビニュース

2017/12/26 12:38:25

日産カナダファイナンス、113万人の顧客データ漏洩の可能性

後藤大地

関連キーワード：情報漏えい

日産カナダファイナンス（NCF; Nissan Canada Finance）は2017年12月21日(米国時間)、「Nissan Canada Finance informs customers of possible data breach - Nissan Online Newsroom」において、同社のカナダの顧客に対して個人情報が漏洩した可能性があることを通知していると発表した。同社およびINFINITI Financial Services Canadaから車輌を購入した顧客が影響を受ける可能性があるという。

日産カナダファイナンスは2017年12月11日(カナダ時間)に個人情報に不正アクセスの痕跡があることを発見。流出した可能性がある個人情報には顧客名、住所、車輌モデル、車輌識別番号、クレジットスコア、融資金額、月々の支払金額などが含まれている可能性があり、どの個人情報が影響を受けるかは現在調査中としている。