【Technical Report18-01】

2018 年 1 月 31 日
株式会社セキュアソフト

注意喚起： CPU 脆弱性 Meltdown,Spectre について

～CPU に対するサイドチャネル攻撃～

1. 概要

2017 年 12 月に Intel 製 CPU および、一部の AMD、ARM 製 CPU において脆弱性が見つりました。対象となる製品が大量にあり、影響範囲が大変大きい問題として、年明けから一般のメディアも含め多数報道されています。
CPU の脆弱性「Meltdown」、「Spectre」は、ほぼすべての PC やスマートフォンが影響を受けます。OS だけでなく、Web ブラウザなどのアプリケーションソフトウェアも対策パッチを適用する必要があり、正しい情報を把握し早期に対策をすることが必要です。

2. Meltdown、Spectre について

Intel、AMD、ARM など、現在の CPU 技術として、処理向上に寄与する投機的実行（speculative execution)プロセスがあり、このプロセスに深刻な脆弱性が存在することが判明しました。この脆弱性を悪用すると、システムメモリのデータを読み取ることができ、パスワードや暗号キーといった機密データを盗まれる可能性があります。
投機的実行プロセスの脆弱性は 2017 年中に Google の Project Zero チームが発見し、Intel、AMD、ARM に報告していました。同チームが収集した情報は「Reading privileged memory with a side-channel」という記事で 1 月 3 日にブログで公開されました。報告されている脆弱性は下記の 3 つです。「Variant 1」と「Variant 2」については「Spectre（スペクター）」、「Variant 3」には「Meltdown（メルトダウン）」という名称がつけられています。

Variant 1（CVE-2017-5753）：境界チェックのバイパス
Variant 2（CVE-2017-5715）：分岐ターゲットのインジェクション
Variant 3（CVE-2017-5754）：不正なデータのキャッシュ読み込み

⑴ Meltdown および Spectre に関する脆弱性概要

① Meltdown

ハードウェアの問題であることが原因で、特権を持たないユーザーが任意のカーネルメモリをダンプすることが可能となる。OS とアプリケーション間における脆弱性となり、実行中の他のプログラムが使用するメモリに保存されている情報（機密情報など）が読み取られる可能性がある。

② Spectre

Meltdown とは異なる脆弱性で、他のプログラムが自プログラムのメモリ内の任意の場所にアクセスするよう仕向けさせることが可能となる。異なるアプリケーション間における脆弱性となり、Meltdown と比べて悪用は難しいとされる。

⑵　攻撃情報

公開時点(1 月 3 日)で悪用情報無し

⑶　対象の製品（CPU とシステム）

①対象 CPU

Meltdown: Intel CPU、一部の ARM 製品

Spectre: Intel、AMD、ARM 各社のプロセッサーに影響

②対象システム

Windows、OS X、Android はじめあらゆる OS プラットフォーム

・Intel 社　本件に関する情報サイト

https://newsroom.intel.com/press-kits/security-exploits-intel-products/

・AMD 社　本件に関する情報サイト

https://www.amd.com/ja/corporate/speculative-execution

⑷　対策方法

根本対策は CPU を交換することになりますが、現実的ではありません。対策パッチなどがハードウェア、ソフトウェア（OS、アプリケーション）と多岐に渡りリリースされています。以下は主要な OS とブラウザの情報です。（1 月 16 日　時点）

■Windows 10

Anniversary Update (1607) 用 KB4056890

Creators Update (1703) 用 KB4056891

Fall Creators Update (1709) 用 KB4056892

Windows 7 用 KB4056897　KB4056894

Windows 8.1 用 KB4056898　KB4056895

■Apple

macOS High Sierra 10.13.2 (Safari の修正含む)

iOS 11.2.2 (Safari/WebKit の修正含む)

■Red Hat

Red Hat Enterprise Linux 7 / CentOS 7

kernel-3.10.0-693.11.6.el7

Red Hat Enterprise Linux 6 / CentOS 6

kernel-2.6.32-696.18.7.el6

■Amazon Linux
kernel-4.9.70-25.242.amzn1

■Firefox
Firefox 57.0.4
Firefox 52.6 ESR

■Safari / WebKit
修正バージョンの OS に含む

■Chrome
Firefox 57.0.4
Firefox 52.6 ESR

⑸　二次的影響について
上記の脆弱性の対策を実施した際に以下のような二次的問題が発生しています。
対策を適用する際には、検証や情報を確認頂き適用することを推奨します。

① Microsoft が提供したパッチを適用すると PC の動作が遅くなる。不安定になるとの報告。
② Intel の一部 CPU 搭載マシン、脆弱性対策パッチ適用でリブート増加（要約）
http://www.itmedia.co.jp/news/spv/1801/15/news058_0.html
③ ウイルス対策ソフト導入環境で Windows Updated 後に BSoD（Blue Screen of Death）発生の可能性

また、「Meltdown」や「Spectre」に対するパッチを偽装したマルウェアの存在も報告されているため、パッチの入手元についても十分な確認が必要です。

⑹　参考情報
https://meltdownattack.com/　（https://spectreattack.com/　も同じ内容です）

CVE
https://nvd.nist.gov/vuln/detail/CVE-2017-5753
https://nvd.nist.gov/vuln/detail/CVE-2017-5715
https://nvd.nist.gov/vuln/detail/CVE-2017-5754

JVN
http://jvn.jp/vu/JVNVU93823979/

3. SecureSoft 製品の対応について

今回の脆弱性に対応する製品として「SecureSoft Sniper シリーズ」についてご紹介します。

■SecureSoft Sniper シリーズ

ネットワークを通過するパケットに対して、様々な角度から詳細な分析を行い、攻撃を検知・遮断する事ができる「防御」のための不正侵入検知・防御システム（IPS：Intrusion Prevention System）です。

Sniper シリーズでは、今回の脆弱性に対応するシグネチャを、2018 年 1 月 17 日付けでリリース致しました。

シグネチャコード	CVE コード	シグネチャ名
3993	CVE-2017-5754	Processor MeltDown Rogue Data Cache Memory Disclosure
3994	CVE-2017-5754	Processor MeltDown Rogue Data Cache Memory Disclosure.A
3995	CVE-2017-5753 CVE-2017-5715	Processor Spectre Allocated Mal Array Info Disclosure
3996	CVE-2017-5753 CVE-2017-5715	Processor Spectre Allocated Mal Array Info Disclosure.A
3997	CVE-2017-5753 CVE-2017-5715	Processor Spectre Via Javascript Kernnel Memory Leakage
3998	CVE-2017-5753 CVE-2017-5715	Processor Spectre Via Javascript Kernnel Memory Leakage.A
3999	CVE-2017-5753 CVE-2017-5715	Processor Spectre Via Javascript Kernnel Memory Leakage.B
4000	CVE-2017-5753 CVE-2017-5715	Processor Speculative Execution Info Disclosure
4001	CVE-2017-5753 CVE-2017-5715	Processor Speculative Execution Info Disclosure.A
4002	CVE-2017-5753 CVE-2017-5715	Processor Speculative Execution Info Disclosure.B
4003	CVE-2017-5753 CVE-2017-5715	Processor Speculative Execution Info Disclosure.C
4004	CVE-2017-5753 CVE-2017-5715	Processor Speculative Execution Info Disclosure.D
4005	CVE-2017-5753 CVE-2017-5715	Processor Speculative Execution Info Disclosure.E

今回のような影響範囲の大きい脆弱性問題では対策パッチなどをすべての対象機器に早期に適用する事は容易ではありません。そこで、今回の脆弱性を利用した攻撃から Sniper を利用して防衛ラインを確立しつつ、システムのアップデートを行うことが有効な対応策となります。また、普段から SOC サービスを利用してシステムのセキュリティログ監視により予兆を早期に発見することで被害を最小限にすることも有効な対策となります。ぜひ、セキュアソフトの製品、サービスを活用ください。

■SecureSoft Sniper シリーズ
https://www.securesoft.co.jp/products/

■SecureSoft S.O.S サービス
https://www.securesoft.co.jp/security/

«お問合せ先»
株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp