

投機的実行機能を持つ CPU に対するサイドチャネル攻撃について (SSB, RSRE)

2018年5月21日にIntel社より以下の脆弱性 (SSB, RSRE) が公表されました。

INTEL-SA-00115

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html>

1. 製品の該非情報、対応方法

今回の脆弱性について、影響を受ける製品は以下の通りです。

●OS/仮想化ソフトウェア製品

- ・OS/仮想化ソフトウェア製品への影響

当該脆弱性による OS/仮想化ソフトウェア製品への影響は、以下の通りです。

#	製品	影響	対応	備考
1	VMware	あり	<p>本問題に対する情報は下記 URL で公開されています。 VMware Response to Speculative Execution security issues, CVE-2018-3639 and CVE-2018-3640 (54951) https://kb.vmware.com/s/article/54951</p> <p>VMware vSphere, Workstation and Fusion updates enable Hypervisor-Assisted Guest Mitigations for Speculative Store Bypass issue. https://www.vmware.com/security/advisories/VMSA-2018-0012.html</p>	
2	Windows Server/Client	あり	<p>本問題に対する情報は下記 URL で公開されています。 ADV180012 Microsoft Guidance for Speculative Store Bypass https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180012</p> <p>ADV180013 Microsoft Guidance for Rogue System Register Read https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV180013</p>	
3	Red Hat Enterprise Linux	あり	<p>本問題に対する情報は下記 URL で公開されています。 Kernel Side-Channel Attack using Speculative Store Bypass - CVE-2018-3639 https://access.redhat.com/security/vulnerabilities/ssbd</p>	
4	AIX Virtual I/O Server	あり	<p>本問題に対する情報は下記 URL で公開されています。 Potential Impact on Processors in the POWER Family https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/</p> <p>Security Bulletin: IBM has released the following fixes for AIX and VIOS in response to Speculative Store Bypass (SSB), also known as Variant 4. http://www-01.ibm.com/support/docview.wss?uid=isg3T1027700</p>	
5	HP-UX	なし	<p>HP-UX について、本脆弱性の影響はありません。 (Intel Itanium プロセッサのため) https://h22208.www2.hp.com/eginfolib/securityalerts/Variant/Variant_Vulnerabilities.html</p>	

●ストレージ管理製品の仮想アプライアンス

以下のストレージ管理製品の仮想アプライアンスにつきましては、出荷形式として VM イメージ形態にて提供しており、ゲスト OS として Oracle Linux を同梱しております。この Oracle Linux は今回の脆弱性の影響を受けます。下記の仮想アプライアンスとも、同梱されている Oracle Linux につきましては、お客様が直接 Oracle 社とサポート契約を締結していただく形となるため、Oracle Linux の対応方法についてのご質問は、Oracle 社のサポートにご確認をお願いします。

#	製品	該当バージョン	影響	備考
1	Hitachi Command Suite 製品の仮想アプライアンス	V8. 4. 1 以降	あり	Oracle Linux に影響あり
2	Hitachi Storage Provider for VMware vCenter の仮想アプライアンス	V3. 3. 0 以降	あり	Oracle Linux に影響あり

2. 本件に関する問い合わせ窓口

各製品のサポート窓口にお問い合わせください。

3. 更新履歴

2018年5月28日：「OS/仮想化ソフトウェア製品への影響」を更新しました。

2018年5月23日：「OS/仮想化ソフトウェア製品への影響」を更新しました。

「ストレージ管理製品の仮想アプライアンス」を追加しました。

2018年5月22日：このセキュリティ情報ページを新規作成および発信しました。

- ・弊社では、セキュリティ対応に関して正確な情報を提供するように努力しておりますが、セキュリティ問題に関する情報は変化しており、当ホームページで記載している内容を予告なく変更することがありますので、あらかじめご了承ください。情報ご参照の際には、常に最新の情報をご確認いただくようお願いします。
- ・当ホームページに記載されている製品には、他社開発製品が含まれております。これらのセキュリティ情報については他社から提供、または公開された情報を基にしております。弊社では、情報の正確性および完全性について注意を払っておりますが、開発元の状況変化に伴い、当ホームページの記載内容に変更が生じることがあります。
- ・当ホームページはセキュリティ情報の提供を目的としたものであり、法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして、弊社では責任を負いかねます。
- ・当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。
- ・記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。