

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 (L1TF, L1 Terminal Fault)

投機的実行機能を持つ Intel 社製 CPU に対してサイドチャネル攻撃により L1 データキャッシュ情報が漏えいする脆弱性 (L1TF, L1 Terminal Fault) が報告されています。

[JVN#97646030 (CVE-2018-3615、CVE-2018-3620、CVE-2018-3646)]

●ソフトウェア製品への影響

CVE-2018-3620 および CVE-2018-3646 によるソフトウェア製品への影響は、以下の通りです。

CVE-2018-3615 については、ソフトウェア製品での対策は必要ありません。

#	製品	影響	対応	備考
1	VMware vSphere	あり	本問題に対する詳細については、以下の URL を参照してください。 VMSA-2018-0020 https://www.vmware.com/security/advisories/VMSA-2018-0020.html アプライアンス製品の本問題に対する詳細は、次の URL を参照してください。 VMSA-2018-0021 https://www.vmware.com/security/advisories/VMSA-2018-0021.html	
2	Windows Server/ Windows Client	あり	本問題に対する詳細については、以下の URL を参照してください。 ADV180018 L1TF バリエーションのリスクを軽減するためのガイダンス https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/adv180018 L1 Terminal Fault から保護するための Windows Server 向けガイダンス https://support.microsoft.com/ja-jp/help/4457951/windows-server-guidance-to-protect-against-l1-terminal-fault	
3	Red Hat Enterprise Linux	あり	本問題に対する詳細については、以下の URL を参照してください。 L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646 https://access.redhat.com/security/vulnerabilities/L1TF	
4	AIX Virtual I/O Server	あり	本問題に対する詳細については、以下の URL を参照してください。 https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/ HWS18-001 (CVE-2017-5754) と同様の対処となります。 http://www.hitachi-support.com/alert/us/HWS18-001/soft.pdf	

●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。

●更新履歴

2018年8月23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できるよう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いたします。
- ・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。