「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

投機的実行機能を持つ CPU に対してサイドチャネル攻撃を行う手法が複数の研究者によって報告されています。
[JVNVU#93823979(CVE-2017-5715、CVE-2017-5753、CVE-2017-5754)]

●OS/仮想化ソフトウェア製品
(1)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 vSphere	あり	本問題に対する対策版が以下URLで公開されています。 https://www.vmware.com/security/advisories/VMSA-2018-0004.html 【注意事項】 1/9公開のESXiのパッチに問題が報告されたため、ESXiのパッチ提供を停止しましたが、3/20に新たなパッチが公開されました。 ESXi のパッチ適用前に、vCenter Server のパッチを適用してください。（詳細は https://kb.vmware.com/s/article/52085 参照） ・アプライアンス製品の本問題に対する対策版が以下URL で公開されています。 https://www.vmware.com/security/advisories/VMSA-2018-0007.html	
2	Windows Server	あり	本問題に対する対策版が以下 URL で公開されています。 https://support.microsoft.com/ja-jp/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution 　本セキュリティアップデートを適用する前に、ウィルス対策ソフトウェアの提供元に対応状況をご確認ください。 　ウィルス対策ソフトが対応していない場合は、ブルースクリーンになるなどの問題が発生する場合があります。 　セキュリティアップデート適用の際には以下の情報も参照してください。 　重要: 2018 年 1 月 4 日にリリースされた Windows セキュリティ更新プログラムとウイルス対策ソフトウェア https://support.microsoft.com/ja-jp/help/4072699/january-3-2018-windows-security-updates-and-antivirus-software 【注意事項(Windows Server 2008 R2(64bit)環境のみ)】 2018 年 1 月以降にリリースされた脆弱性対策パッチの適用後、特権のないプロセスが Windows カーネルで使用可能なメモリスペース全体を読み書きできてしまう問題が報告されています。本問題は、KB4100480 で対策されています。あわせて適用をご検討下さい。 （詳細は https://support.microsoft.com/en-us/help/4100480/windows-kernel-update-for-cve-2018-1038 参照）	

3	Windows Client	あり	本問題に対する対策版が以下URLで公開されています。 https://support.microsoft.com/ja-jp/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in 本セキュリティアップデートを適用する前に、ウィルス対策ソフトウェアの提供元に対応状況をご確認ください。 ウィルス対策ソフトが対応していない場合は、ブルースクリーンになるなどの問題が発生する場合があります。 セキュリティアップデート適用の際には以下の情報も参照してください。 重要: 2018 年1 月4 日にリリースされたWindows セキュリティ更新プログラムとウイルス対策ソフトウェア https://support.microsoft.com/ja-jp/help/4072699/january-3-2018-windows-security-updates-and-antivirus-software 【注意事項(Windows 7(64bit)環境のみ)】 2018 年 1 月以降にリリースされた脆弱性対策パッチの適用後、特権のないプロセスが Windows カーネルで使用可能なメモリスペース全体を読み書きできてしまう問題が報告されています。本問題は、KB4100480 で対策されています。あわせて適用をご検討下さい。 （詳細は https://support.microsoft.com/en-us/help/4100480/windows-kernel-update-for-cve-2018-1038 参照）	
4	Red Hat Enterprise Linux	あり	本問題に対する対策版は以下 URL で公開されています。 Red Hat 社： https://access.redhat.com/security/vulnerabilities/speculativeexecution 本対策版を含んだ改良版メディアについては、下記の日程で提供可能になります。 ・RHEL7: RHEL7.4 の改良版メディア （2018 年 2 月末より） ・RHEL6: RHEL6.9 の改良版メディア （2018 年 2 月末より） 対策をご検討のお客様はサポートサービス窓口へご連絡ください。	
5	AIX Virtual I/O Server	あり	対策パッチ(IFIX)は、次の IBM のサイト情報を参照の上、ダウンロードしてください。 Security Bulletin: IBM has released AIX and VIOS iFixes in response to the vulnerabilities known as Spectre and Meltdown. http://www-01.ibm.com/support/docview.wss?uid=isg3T1026912 対策パッチ(IFIX)を適用するための前提となる AIX、VIOS のバージョンは次の通りとなります。 ・AIX V7.2 TL0SP5 (AIX Level 7.2.0.5) 日立バージョン： AIX V7.2 01-00-/B(予防保守パッチ 01-00-SB) ・AIX V7.1 TL4SP5 (AIX Level 7.1.4.5) 日立バージョン： AIX V7.1 01-04-/A(予防保守パッチ 01-04-SB) ・AIX V6.1 TL9SP10 (AIX Level 6.1.9.10) 日立バージョン： AIX V6.1 01-09-/F(予防保守パッチ 01-09-SG) ※対策パッチ(IFIX)を同梱して提供中。 ・Virtual I/O Server (VIOS Level 2.2.5.10) 日立バージョン：Virtual I/O Server V2.2 01-10 また、本問題の対策を含む AIX 及び Virtual I/O Server の製品（予防保守パッチ）リリース時期については 2018 年 3 月より順次公開予定です。	
6	SQL Server	あり	本問題に対する対策版が以下 URL で公開されています。 https://support.microsoft.com/ja-jp/help/4073225/guidance-for-sql-server	
7	HP-UX	なし	HP-UX については、本脆弱性の影響はありません。 以下に HPE 社の情報が公開されています。	

			https://support.hpe.com/hpsc/doc/public/display?sp4ts.oid=null&docLocale=en_US&docId=emr_na-a00039267en_us	
8	Citrix XenDesktop / XenApp	なし	XenDesktop / XenApp については、本脆弱性の影響はありません。 以下に Citrix 社の情報が公開されています。 https://support.citrix.com/article/CTX231399	

(2) OS/仮想化ソフトウェア製品のパッチ適用による性能への影響
各ソフトウェア製品のパッチ適用における性能への影響は、以下の通りです。
各ベンダのサイト情報を元に、お客様システムへの影響をご確認ください。

#	製品	影響	備考
1	VMware vSphere	VMware の下記サイトにて性能影響についての記載があります。 https://kb.vmware.com/s/article/52337	
2	・Windows Server ・Windows Client	Microsoft の下記サイトにて性能影響についての記載があります。 https://blogs.technet.microsoft.com/jpsecurity/2018/01/23/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/	
3	Red Hat Enterprise Linux	Red Hat の下記サイトにて性能影響についての記載があります。 https://access.redhat.com/ja/node/3315851	
4	AIX Virtual I/O Server	サポート窓口へお問い合わせください。	
5	SQL Server	Microsoft の下記サイトにて性能影響についての記載があります。 https://support.microsoft.com/ja-jp/help/4073225/guidance-for-sql-server	

●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

●サーバ管理製品
以下のサーバ管理製品につきましては SQL Server(Express エディション)を同梱しており、管理サーバへの製品インストール時に SQL Server もインストールされます。この SQL Server は今回の脆弱性の影響を受けます。修正パッチについては、Microsoft 社から入手していただくこととしております。SQL Server への脆弱性による影響については、「(1)OS/仮想化ソフトウェア製品への影響の#6」 および「(2) OS/仮想化ソフトウェア製品のパッチ適用による性能への影響の#5」にある「SQL Server」の記載を参照願います。

#	製品	該当バージョン	影響	備考
1	JP1/ServerConductor/Deployment Manager	V08-50 以降	あり	SQL Server に影響あり
2	Hitachi Compute Systems Manager (Deployment Manager Plug-in)	V7.4.1-02 以降	あり	SQL Server に影響あり

●本件に関する問い合せ窓口
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 4 月 13 日：「OS/仮想化ソフトウェア製品のパッチ適用による性能への影響」を更新しました。
2018 年 4 月 3 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 3 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。
2018 年 3 月 9 日：「 OS/仮想化ソフトウェア製品への影響」「OS/仮想化ソフトウェア製品のパッチ適用による性能への影響」を更新しました。
2018 年 3 月 1 日：「サーバ管理製品」の情報を追加しました。
2018 年 2 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。
2018 年 2 月 16 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 2 月 9 日：「 OS/仮想化ソフトウェア製品への影響」「OS/仮想化ソフトウェア製品のパッチ適用による性能への影響」を更新しました。
2018 年 2 月 5 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 1 月 31 日：「 OS/仮想化ソフトウェア製品への影響」「OS/仮想化ソフトウェア製品のパッチ適用による性能への影響」を更新しました。
2018 年 1 月 26 日：「ストレージ管理製品の仮想アプライアンス」の情報を追加しました。
2018 年 1 月 24 日：「パッチ適用による性能への影響」の Windows Server/Client に関し、Microsoft 社の日本語サイトを掲載しました。
2018 年 1 月 17 日：「パッチ適用による性能への影響」の情報を追加しました。また、AIX 対策版の発行予定日を改訂しました。
2018 年 1 月 16 日：Windows Client の情報を追加しました。
2018 年 1 月 15 日：VMware vSphere の情報を更新しました。
2018 年 1 月 11 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。