KDDIクラウドプラットフォームサービス(KCPS)
CPU脆弱性(Meltdown/Spectre)に対する
パッチ適用・確認手順書_Linux OS(RHEL・CentOS)

KCPS ver.1の手順書となります

はじめに

本資料は、KDDIクラウドプラットフォームサービス(以下、KCPS)ナレッジサイトにおいて情報を発出している「KCPSに関するMeltdownおよびSpectre脆弱性への対応ついて」に関する、お客さまのインスタンス(仮想サーバー)上のLinux OS(Red Hat Enterprise Linux(以下、RHEL)及びCentOS)への脆弱性対応手順です。

第6報
https://iaas.cloud-platform.kddi.ne.jp/information/vulnerability/24186/

※過去のご案内内容につきましては、以下をご参照ください。

第１報
https://iaas.cloud-platform.kddi.ne.jp/information/vulnerability/20780/

第２報
https://iaas.cloud-platform.kddi.ne.jp/information/vulnerability/21944/

第３報
https://iaas.cloud-platform.kddi.ne.jp/information/vulnerability/21986/

第４報
https://iaas.cloud-platform.kddi.ne.jp/information/vulnerability/22424/

第5報
https://iaas.cloud-platform.kddi.ne.jp/information/vulnerability/22649/

お客さまにはお手数をお掛けしますが、次ページ以降の内容をご一読の上、実施可否をご検討ください。

お客さまのインスタンスへの影響

ご利用中のお客さま限り

弊社試験にてお客さまご利用のインスタンスのOSにCPU脆弱性に対するパッチを適用することでインスタンスのパフォーマンスに影響がある事を確認しております。

お客さまのシステムで発生するパフォーマンスへの影響を評価の上、ご適用頂きますよう宜しくお願い申し上げます。

<ご参考>

◇投機的実行の脆弱性によるパフォーマンスへの影響 - CVE-2017-5754、CVE-2017-5753、および CVE-2017-5715 に対するセキュリティーパッチによるパフォーマンスへの影響
https://access.redhat.com/ja/articles/3315851

◇カーネルのサイドチャネル攻撃 - CVE-2017-5754 CVE-2017-5753 CVE-2017-5715
https://access.redhat.com/ja/security/vulnerabilities/3311961

パッチ適用後に元(以前)の状態に戻すはできませんので、本ページの影響度をご参照の上、パッチ適用要否をお客さまにてご検討頂けますよう、宜しくお願いいたします。

脆弱性対応_手順

①対象のインスタンスにrootでsshログインする

②下記コマンドにて、対象OSのカーネルアップデートを行う
※対象OSのカーネルが最新となりますのでご注意ください。
【実行コマンド】

```
# yum update kernel
```

※ダウンロードサイズの確認を問われるため「y」を押下する
※エラー無く正常に完了すること

③インスタンスの”停止/起動”を実施

※アップデートを反映させるため、Admin Consoleからの”停止/起動”が必須となります。

脆弱性対応_確認手順①

本手順は前述の脆弱性対応手順が正常に実行されたことを確認するための手順です。

①AdminConsoleから脆弱性対応のスクリプトを入手する

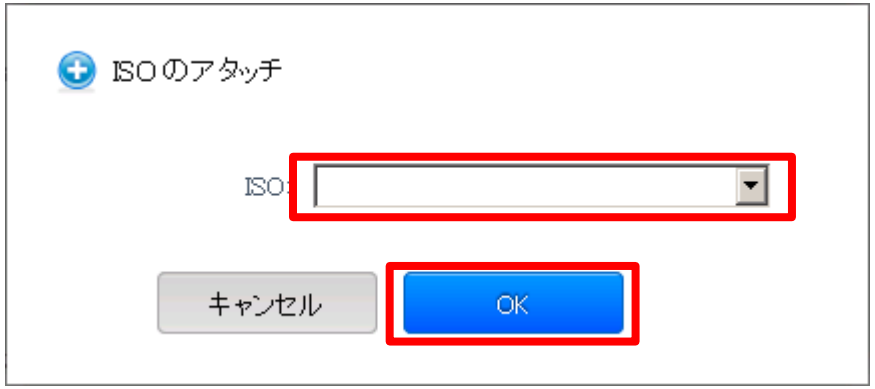
1．対象インスタンスへISOをアタッチ※する

※ ISOのアタッチ方法は、以下URLをご参照ください。
https://iaas.cloud-platform.kddi.ne.jp/virtual-server/storage/iso/attach-detach/

脆弱性対応_確認手順②

②プルダウンメニューより、対象のISOを選択し、「OK」押下

ISO名：Spectre_Meltdown_CheckScript.iso



脆弱性対応_確認手順③-④

③対象インスタンスにrootでsshログインする

④項番②でアタッチしたISOをmountする

※実行例(mount先ディレクトリ等は任意です)

1．スクリプト保存先ディレクト作成

```
# mkdir /meltdown_spectre_script
```

2．mount実施

```
# mount /dev/cdrom /media/
```

※読み込み専用でマウントする旨のメッセージが出力される

3．mount用ディレクトにファイルをコピーする

```
# cp -p /media/01_Linux/spectre-meltdown-checker.sh /meltdown_spectre_script
```

4．コピー先ディレクトへ移動

```
# cd /meltdown_spectre_script/
```

脆弱性対応_確認手順⑤-⑥

⑤スクリプトを実行する

```
# ./spectre-meltdown-checker.sh
```

⑥実行結果を確認する

・次ページの「スクリプト実行結果例」のように、
CVF-2017-5753、CVF-2017-5715、CVF-2017-5754の３つの脆弱性について、
「STATUS」項目が「NOT VULNERABLE」となっていることを確認する

スクリプト実行結果例


```
CVE-2017-5753 [bounds check bypass] aka 'Spectre Variant 1'
* Mitigated according to the /sys interface: YES (Mitigation: Load fences)
* Kernel has array_index_mask_nospec (x86): NO
* Kernel has the Red Hat/Ubuntu patch: YES
* Kernel has mask_nospec64 (arm): NO
> STATUS: NOT VULNERABLE (Mitigation: Load fences)

CVE-2017-5715 [branch target injection] aka 'Spectre Variant 2'
* Mitigated according to the /sys interface: NO (Vulnerable: Retpoline with un
safe module(s))
* Mitigation 1
  * Kernel is compiled with IBRS support: YES
    * IBRS enabled and active: NO
  * Kernel is compiled with IBPB support: YES
    * IBPB enabled and active: YES
* Mitigation 2
  * Kernel has branch predictor hardening (arm): NO
  * Kernel compiled with retpoline option: YES
    * Kernel compiled with a retpoline-aware compiler: YES (kernel reports ful
l retpoline compilation)
    * Retpoline is enabled: YES
> STATUS: NOT VULNERABLE (Full retpoline + IBPB are mitigating the vulnerabili
ty)

CVE-2017-5754 [rogue data cache load] aka 'Meltdown' aka 'Variant 3'
* Mitigated according to the /sys interface: YES (Mitigation: PTI)
* Kernel supports Page Table Isolation (PTI): YES
  * PTI enabled and active: YES
  * Reduced performance impact of PTI: YES (CPU supports PCID, performance imp
act of PTI will be reduced)
* Running as a Xen PV DomU: NO
> STATUS: NOT VULNERABLE (Mitigation: PTI)
```

脆弱性対応_確認手順⑦-⑨

⑦作業用に作成したディレクトを削除する
※本手順では「meltdown_spectre_script」ディレクトリ

```
# rm -r /meltdown_spectre_script/
```

⑧ISOのunmountを実施する

```
# umount /dev/cdrom
```

⑨AdminConsoleより、以下ISOをデタッチ※する

ISO名：Spectre_Meltdown_CheckScript.iso

※ ISOのデタッチ方法は、以下URLをご参照ください。
https://iaas.cloud-platform.kddi.ne.jp/virtual-server/storage/iso/attach-detach/


Designing The Future
KDDI