Openfind Software Engineered for Growth

Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-18-001

Openfind 郵件安全威脅與潛在資安風險通報

Openfind 專注於郵件安全領域已經有 20 年以上的豐富經驗，致力提供客戶穩定、安全、可靠的郵件安全系統與服務。為提昇客戶郵件安全意識與避免潛在資安風險擴大，Openfind 郵件安全研究團隊將不定期提供客戶有關郵件安全威脅的即時訊息，以及潛在資安風險的警示通報。

如果您在使用 Openfind 各項產品時，有發現任何郵件安全威脅或潛在資安風險，也歡迎您透過 support@openfind.com.tw 與我們聯繫。Openfind 技術團隊將提供您即時的資安諮詢與更新服務。

公告日期：2018 / 1 / 15

威脅類別： CPU 漏洞

威脅程度：3 (分數 1~5，5 代表資安事件威脅程度很高)

影響產品版本： Openfind 全產品

事件摘要：

Google Project Zero 近來揭發 CPU 的「推測執行」（speculative execution）安全漏洞，經研究人員實際檢測後歸納出兩大攻擊手法，分別為 Meltdown 與 Spectre。目前已針對這兩類攻擊手法發出 3 個變種漏洞的 CVE 通報，分別為漏洞編號 CVE-2017-5754、CVE-2017-5753 與 CVE-2017-5715。Meltdown 與 Spectre 都是利用推測執行造成的處理器設計弱點所發動的攻擊方式，因此所有使用 Intel CPU 的伺服器都有機會受到影響，目前 Red Hat 官方也已提供修正問題的更新修補程式。

針對此次的漏洞及官方提供的更新修補程式，因 Openfind 產品**不容許**任何形式的未授權代碼執行，故我們受攻擊的機率極低，但為阻絕任何第三方套件所帶來的風險，此次 Openfind 仍將主動整理作業系統的官方資料並提供更新說明，讓客戶可快速更新各產品所使用的作業系統環境。

建議措施：

建議所有 Openfind 產品客戶立即更新各作業系統之官方所提供的安全性修正程式，以阻絕任何潛在性風險。

更新方式：

Openfind 全產品之客戶，可按照下列各產品的說明進行更新，或透過聯繫 Openfind 技術服務團隊，以協助進行更新事宜。

- **Openfind 全產品客戶**
  - RedHat Linux 官方弱點公告：
    https://access.redhat.com/security/vulnerabilities/speculativeexecution
  - 修正此弱點僅需更新作業系統核心 (OS Kernel)，Openfind 產品不需要更新。
  - 作業系統核心更新方法：
    1. 檢測是否為最新版

       $ uname -r

       2.6.32-573.26.1.el6.x86_64

       ```
       [root@c82 ~]# uname -r
       2.6.32-573.26.1.el6.x86_64
       ```

    2. 更新指令

       $ sudo yum install -y kernel

       ```
       [root@new webmail]# yum install -y kernel
       Loaded plugins: fastestmirror
       Setting up Install Process
       Loading mirror speeds from cached hostfile
        * base: linux.cs.nctu.edu.tw
        * epel: ftp.cuhk.edu.hk
        * extras: linux.cs.nctu.edu.tw
        * remi-safe: mirrors.thzhost.com
        * updates: linux.cs.nctu.edu.tw
       ```

    3. 重新啟動系統並確認是否安裝成功

       $ reboot

       ```
       [root@c82 ~]# reboot

       Broadcast message from root@c82.training.lab
               (/dev/pts/0) at 13:54 ...

       The system is going down for reboot NOW!
       ```

       $ uname -r

       2.6.32-696.18.7.el6.x86_64

       ```
       [root@c82 ~]# uname -r
       2.6.32-696.18.7.el6.x86_64
       ```

4. 驗證 3 個 CVE

$ rpm -q --changelog kernel | egrep 'CVE-2017-5715|CVE-2017-5753|CVE-2017-5754'

- [x86] spec_ctrl: svm: spec_ctrl at vmexit needs per-cpu areas functional (Waiman Long) [1519797 1519796] {CVE-2017-5715}

- [x86] spec_ctrl: Eliminate redundnat FEATURE Not Present messages (Waiman Long) [1519797 1519796] {CVE-2017-5715}

……..

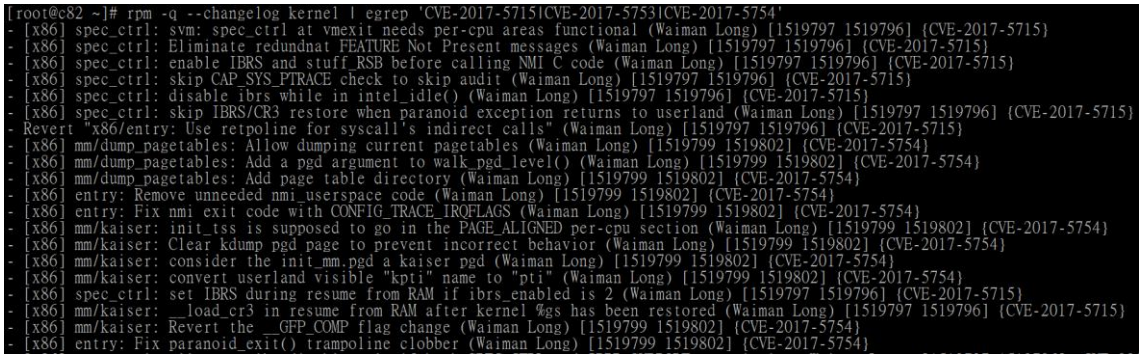
- [x86] entry: Remove trampoline check from paranoid entry path (Waiman Long) [1519799 1519802] {CVE-2017-5754}

- [x86] entry: Don't switch to trampoline stack in paranoid_exit (Waiman Long) [1519799 1519802] {CVE-2017-5754}

……..

- [x86] cpu/AMD: Remove now unused definition of MFENCE_RDTSC feature (Waiman Long) [1519787 1519789] {CVE-2017-5753}

- [x86] cpu/AMD: Make the LFENCE instruction serialized (Waiman Long) [1519787 1519789] {CVE-2017-5753}



- **ArkEasePro 客戶**

  請直接聯繫 Openfind 技術服務團隊進行以下更新：

  - 2.6.2 以前版本之客戶，建議升級至 2.7.2 版。
  - 目前為 2.7.2 版之客戶將提供 2.7.3 版 (預計為本月底後提供)。

關於 Openfind 電子郵件威脅實驗室

隨著資訊安全威脅日益升高，所有資訊系統都面臨相當嚴峻的挑戰。其中，電子郵件系統更是諸多資安威脅中首當其衝的主要標的。由於資訊安全的範圍相當廣泛與多元，在實際的案例中，客戶只需要定期更新 Patch 與升級系統，結合 Openfind 主動式安全偵測服務，便可避免暴露於風險之中。Openfind 本著服務客戶的精神，不但會繼續強化產品在資安上的防護與感知能力，也會持續嚴格監控產品的安全。Openfind 電子郵件威脅實驗室也會不定期更新網路上重大的電子郵件安全威脅訊息，幫助管理者掌握最新的資安趨勢與脈動。