行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2018-0001	發布時間	Wed Jan 10 17:16:30 CST 2018
事件類型	漏洞預警	發現時間	Wed Jan 10 00:00:00 CST 2018
警訊名稱	[更新-影響等級]多款 CPU 處理器存在 Meltdown 與 Spectre 漏洞，允許攻擊者在受害系統上讀取記憶體內的機敏資訊，請儘速評估確認與進行修正		
內容說明	Google Project Zero 等研究團隊於 1 月 3 日揭露 Meltdown 與 Spectre 兩種透過推測執行(Speculative execution)的攻擊方式，目前已知該攻擊方式至少須具備受害系統的一般使用者權限，或是誘騙受害者去觸發惡意程式等方式。 若具以上前提條件，則其中 Meltdown(CVE-2017-5754)漏洞，有機會允許攻擊者以系統權限讀取應用程式與作業系統所用到的部分記憶體，而 Spectre (CVE-2017-5753)與(CVE-2017-5715)漏洞，則允許攻擊者讀取 CPU 核心內的快取檔資料，或有機會取得執行中的應用程式儲存在記憶體內的機敏資訊。		
影響平台	Intel 處理器： -Intel Core i3 processor (45nm and 32nm) -Intel Core i5 processor (45nm and 32nm) -Intel Core i7 processor (45nm and 32nm) -Intel Core M processor family (45nm and 32nm) -2nd generation Intel Core processors -3rd generation Intel Core processors -4th generation Intel Core processors -5th generation Intel Core processors		

	-6th generation Intel Core processors -7th generation Intel Core processors -8th generation Intel Core processors -Intel Core X-series Processor Family for Intel X99 platforms -Intel Core X-series Processor Family for Intel X299 platforms -Intel Xeon processor 3400 series -Intel Xeon processor 3600 series -Intel Xeon processor 5500 series -Intel Xeon processor 5600 series -Intel Xeon processor 6500 series -Intel Xeon processor 7500 series -Intel Xeon Processor E3 Family -Intel Xeon Processor E3 v2 Family -Intel Xeon Processor E3 v3 Family -Intel Xeon Processor E3 v4 Family -Intel Xeon Processor E3 v5 Family -Intel Xeon Processor E3 v6 Family -Intel Xeon Processor E5 Family -Intel Xeon Processor E5 v2 Family -Intel Xeon Processor E5 v3 Family -Intel Xeon Processor E5 v4 Family

	-Intel Xeon Processor E7 Family -Intel Xeon Processor E7 v2 Family -Intel Xeon Processor E7 v3 Family -Intel Xeon Processor E7 v4 Family -Intel Xeon Processor Scalable Family -Intel Xeon Phi Processor 3200, 5200, 7200 Series -Intel Atom Processor C Series -Intel Atom Processor E Series -Intel Atom Processor A Series -Intel Atom Processor x3 Series -Intel Atom Processor Z Series -Intel Celeron Processor J Series -Intel Celeron Processor N Series -Intel Pentium Processor J Series -Intel Pentium Processor N Series ARM： -Cortex-R7 -Cortex-R8 -Cortex-A8 -Cortex-A9 -Cortex-A15

	-Cortex-A17 -Cortex-A57 -Cort Windows 10ex-A72 -Cortex-A73 -Cortex-A75
影響等級	中
建議措施	1. Windows 7/8/10 與 Server 2008/2008R2/2012/2012R2 作業系統，適用以下方法確認是否使用的 CPU 處理器易遭受 Meltdown 與 Spectre 漏洞的攻擊： (1)首先透過微軟官方(https://gallery.technet.microsoft.com/scriptcenter/Speculation-Control-e36f0050#content)網址下載檔案，並將「SpeculationControl.zip」檔案解壓縮 (2)透過搜尋列表搜尋 Windows PowerShell，然後以系統管理員權限執行。 (3)在 Windows PowerShell 視窗切換到檔案解壓縮的位置。 (4)輸入「$SaveExecutionPolicy=Get-ExecutionPolicy」。 (5)輸入「Set-ExecutionPolicy RemoteSigned -Scope Currentuser」→按下 Enter→按下 Y。 (6)輸入「Import-Module .\SpeculationControl.psm1」→按下 Enter→按下 R。 (7)輸入「Get-SpeculationControlSettings」→按下 Enter。 (8)視窗顯示紅字的部分代表可能易遭受攻擊的方式，綠字的部分則代表不受該攻擊方式的影響。 (9)最後確認完畢後，輸入「Set-ExecutionPolicy $SaveExecutionPolicy -Scope Currentuser」→Enter→按下 Y，將 PowerShell 模式復原。 2. Ubuntu/Debian 的 Linux 作業系統可透過以下方法，確認是否使用的 CPU 處理器易遭受 Meltdown 與 Spectre 漏洞的攻擊，其餘開源或商業 Linux 系統則請洽詢維運廠商。 (1)首先可至(https://github.com/speed47/spectre-meltdown-checker)網址下載 Linu

x 的檢查檔案。

(2)下載方式，打開終端視窗，輸入「git clone https://github.com/speed47/spectre-meltdown-checker.git」或「wget https://raw.githubusercontent.com/speed47/spectre-meltdown-checker/master/spectre-meltdown-checker.sh」。

(3)接著切換到下載檔案的位址，並以管理者模式運行檢查檔案「sudo spectre-meltdown-checker.sh」。

(4)可檢視結果中的 STATUS 狀態(VULNERABLE 或 NOT VULNERABLE)，確認當前是否易遭受 Meltdown 與 Spectre 漏洞的影響。

3.目前部分廠商已針對部分產品或設備釋出更新，可參考或持續關注以下各家廠商的專區進行確認：

作業系統更新：

-Microsoft Windows:

(1)確認作業系統版本。

(2)下載作業系統的更新檔: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

-APPLE：https://support.apple.com/en-us/HT201222

(1)macOS High Sierra: 至 App Store，點選更新項目，更新 macOS High Sierra 10.13.2 Supplemental Update。

(2)OS X El Capitan 10.11.6 and macOS Sierra 10.12.6: 更新 Safari 至 11.0.2。

-iOS: 更新至 iOS 11.2.2。

-VMware：

(1)確認 ESXi、Workstation、Fusion 版本。

(2)至官網下載更新檔: https://www.vmware.com/tw/security/advisories/VMSA-2

	018-0002.html -Ubuntu： (1)確認作業系統版本。 (2)更新核心與套件如網站表格: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/ -RedHat： (1)確認作業系統版本。 (2)至下列網站: https://access.redhat.com/security/vulnerabilities/speculativeexecution ，切換標籤至 Resolve。 (3)更新核心與套件如網站表格。 -SUSE： (1)確認作業系統版本。 (2)更新核心與套件: https://www.suse.com/support/kb/doc/?id=7022512 -Android：確認 Android Security Patch 為一月（等候各原廠系統 OTA 更新檔釋出） 瀏覽器更新： -Edge and IE：同 Microsoft Windows 作業系統更新項目 -Google：https://support.google.com/faqs/answer/7622138 (1)Google chrome Desktop: 更新版本至 63 以上 (2)Google chrome Android: 開啟 Chrome app 於網址列輸入 chrome://flags，確認”Strict site isolation”項目為“Enable” (3)Google chrome iOS: 將 iOS 更新至 11.2.2 以上 -Mozilla Firefox：更新版本至 57.0.4 以上
參考資料	1.https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.h

	tml 2.https://www.ithome.com.tw/news/120312 3.https://www.bleepingcomputer.com/news/microsoft/how-to-check-and-update-windows-systems-for-the-meltdown-and-spectre-cpu-flaws/ 4.http://www.kb.cert.org/vuls/id/584653 5.http://technews.tw/2018/01/05/about-intel-meltdown-spectre/

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw