

張貼日期：2015/07/28

轉發漏洞/資安訊息警訊

主旨：【漏洞預警】Hacking Team資料外洩事件最新發現：微軟零時差漏洞CVE-2015-2426

說明：

- 轉發 趨勢科技 漏洞/資安訊息警訊

過去數週，因為近期Hacking Team的資料外洩事件，爆發出為數眾多的零時差漏洞。其中，最新發現的嚴重的漏洞「CVE-2015-2426」牽涉範圍及於Windows的數個版本，如果此漏洞遭到攻擊，可提升Windows本機權限「LPE, Local Privilege Escalation」如此一來，攻擊者可在取得權限後，以rootkit或bootkit感染受害者系統而且不會有任何通知或警訊，最後取得控制權。

因為此漏洞的特性，稍早的Windows版本，即便微軟已不支援，仍有很大可能受到攻擊，包括Windows XP及Windows Server 2000但因微軟早已不支援這些版本的Windows作業系統，因此沒有發布任何消息也沒有釋出安全性更新。

- 影響平台：

1. Windows Server 2003 (微軟稍早已停止支援此版本，但仍將其列在受影響名單中)
2. Windows Vista
3. Windows Server 2008 (+R2)
4. Windows 7, Windows 8/8.1
5. Windows Server 2012 (+R2)
6. Windows RT/RT 8.1
7. Server Core installation options (for Server 2008/2012)

- 建議措施：

微軟已將此漏洞列為Critical等級「MS15-078」並針對此特別在八月的更新日之前釋出了一個安全性更新。趨勢科技與微軟強烈呼籲儘速安裝此更新。

- 參考資料：

Microsoft「<https://technet.microsoft.com/en-us/library/security/MS15-078>
TrendMicro「<http://bit.ly/1g1SAjg>

計算機與通訊中心
網路系統組 敬啟

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/mailling:announcement:20150728_02

Last update: **2016/01/21 15:42**

