GovCERT.HK

Weekly IT Security News Bulletin, 2017-W39

25 September – 1 October 2017

Headlines

Security flaw in Wi-Fi chipset threatening iOS and Android devices

- The Broadcom Wi-Fi System-on-Chip (SoC) firmware is found vulnerable to remote code execution by attackers on the same Wi-Fi network of the targeted device.
- A Google Project Zero security researcher discovered that the vulnerability could be exploited when specially crafted Wi-Fi frames were sent to the Wi-Fi SoC to perform read/write operations, thanks to insufficient validation at its heap buffer. Proof-of-concept (PoC) code was released to illustrate the feasibility to implant a backdoor on iPhone 7 with the vulnerability.
- Apple devices with iOS version prior to 11 and Android devices with security patch level before 5th September 2017 are vulnerable. Apple iOS 11 or above has fixed the issue. Android users have to wait for patches from the device manufacturers. Some de-supported mobile devices, which do not support the latest mobile operating systems, such as iPhone 5 or below, may never be patched.

Advice

- Upgrade to the latest iOS or Android operating systems available for your mobile devices.
- Replace de-supported devices with supported technology to ensure that security updates are provided.
- Do not connect to any untrusted or public Wi-Fi network before patching your devices. "Forget" those saved Wi-Fi network settings on the device to prevent from automatically connecting to a Wi-Fi network.

Sources

- Google Project Zero
- Google Android Security Bulletin
- Apple Security Updates

手機流動支付金有被盜用風險

- 香港中文大學的資訊保安研究團隊公布一項研究結果，發現最為業界採用的三種流動支付技術，包括二維碼（QR code）掃描，磁條讀卡器驗證（magnetic secure transmission）和聲波轉化（audio pay），均存有保安漏洞。不法分子可以在交易過程中，盜取用作驗證付款的支付令牌（payment token），並利用該支付令牌進行未經授權的交易，使用戶蒙受金錢損失。

- 二維碼掃描為現時較為普及的流動支付技術。這種支付技術會在交易時，產生一個二維碼，作為支付令牌。研究報告指出，不法分子可以通過在流動裝置執行惡意軟件，讓用戶無法以原有的二維碼完成交易，而原有的二維碼則由惡意軟件經流動裝置的相機盜取，並從網絡傳送到不法分子手中，用於另一宗交易上圖利。

- 報告亦指出，磁條讀卡器驗證的流動支付技術所產生的磁場訊號，在遠至距離接收器兩米範圍的地方也能夠接收到，不法分子因而可以在交易現場附近，破壞原有交易，竊取並盜用其發出的支付令牌。而常用於自動售賣機的聲波轉化支付技術都發現類似的漏洞，當流動裝置發出聲波，將支付令牌傳送給自動售賣機時，聲波同樣易於被截取，令用戶招致損失。

- 由於這三種流動支付技術皆屬單向式通訊，收款方無法通知付款用戶原有交易失敗，付款用戶不能夠主動取消已發出的支付令牌，電子錢包無聲無色地被盜用。研究團隊已經向有關流動支付服務供應商反映研究結果，讓有關方面採取適當措施，修補保安漏洞。

Advice

- 切勿為流動裝置的操作系統進行越獄（jailbreaking）或破解（rooting），以減低被黑客入侵的機會。

- 安裝並啟動抗惡意程式碼軟件，並定期為抗惡意程式碼軟件本身及其定義檔進行更新。

- 安裝流動應用程式前，用戶應須細閱其存取權限。如要求的權限及功能不相符，應小心考慮是否給予權限，甚至放棄安裝。

- 使用支援雙向式通訊的流動支付技術，如近場通訊（NFC）是其中一種較普及的雙向式通訊技術。

Sources

- 香港中文大學
- USENIX
- 明報

Product Vulnerability Notes & Security Updates

1. **Apple iOS, MacOS and iCloud**
   https://support.apple.com/kb/HT208102
   https://support.apple.com/kb/HT208142
   https://support.apple.com/kb/HT208143
   https://support.apple.com/kb/HT208144
   https://www.hkcert.org/my_url/en/alert/17092701

2. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-cc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-cip
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-dhcp
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ike
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ios-xe
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-lisp
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-nat
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ngwc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-pnp
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-privesc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-profinet
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-rbip-dos
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-restapi
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-vpls

3. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-September/022548.html

4. **Debian**
   https://www.debian.org/security/2017/dsa-3983
   https://www.debian.org/security/2017/dsa-3984
   https://www.debian.org/security/2017/dsa-3985

5. **F5 Products**
   https://support.f5.com/csp/article/K55444705
   https://support.f5.com/csp/article/K82455382

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201709-15
   https://security.gentoo.org/glsa/201709-16
   https://security.gentoo.org/glsa/201709-17
   https://security.gentoo.org/glsa/201709-18
   https://security.gentoo.org/glsa/201709-19
   https://security.gentoo.org/glsa/201709-20
   https://security.gentoo.org/glsa/201709-21
   https://security.gentoo.org/glsa/201709-22
   https://security.gentoo.org/glsa/201709-23
   https://security.gentoo.org/glsa/201709-24
   https://security.gentoo.org/glsa/201709-25
   https://security.gentoo.org/glsa/201709-26
   https://security.gentoo.org/glsa/201709-27

7. **IBM Products**
   http://www-01.ibm.com/support/docview.wss?uid=swg22005235
   http://www-01.ibm.com/support/docview.wss?uid=swg22005596
   http://www-01.ibm.com/support/docview.wss?uid=swg22008025
   http://www-01.ibm.com/support/docview.wss?uid=swg22008918

8. **Mozilla Firefox**
   https://www.mozilla.org/en-US/security/advisories/mfsa2017-21/
   https://www.mozilla.org/en-US/security/advisories/mfsa2017-22/

9. **openSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-09/msg00082.html

10. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-2788.html
    https://linux.oracle.com/errata/ELSA-2017-2789.html
    https://linux.oracle.com/errata/ELSA-2017-2790.html
    https://linux.oracle.com/errata/ELSA-2017-2791.html
    https://linux.oracle.com/errata/ELSA-2017-2795.html
    https://linux.oracle.com/errata/ELSA-2017-2831.html
    https://linux.oracle.com/errata/ELSA-2017-2832.html
    https://linux.oracle.com/errata/ELSA-2017-3626.html

11. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:2792
    https://access.redhat.com/errata/RHSA-2017:2793
    https://access.redhat.com/errata/RHSA-2017:2794
    https://access.redhat.com/errata/RHSA-2017:2795
    https://access.redhat.com/errata/RHSA-2017:2796
    https://access.redhat.com/errata/RHSA-2017:2797
    https://access.redhat.com/errata/RHSA-2017:2798
    https://access.redhat.com/errata/RHSA-2017:2799
    https://access.redhat.com/errata/RHSA-2017:2800
    https://access.redhat.com/errata/RHSA-2017:2801
    https://access.redhat.com/errata/RHSA-2017:2802
    https://access.redhat.com/errata/RHSA-2017:2808
    https://access.redhat.com/errata/RHSA-2017:2809
    https://access.redhat.com/errata/RHSA-2017:2810
    https://access.redhat.com/errata/RHSA-2017:2811
    https://access.redhat.com/errata/RHSA-2017:2831
    https://access.redhat.com/errata/RHSA-2017:2832

12. **Siemens Ruggedcom ROS, SCALANCE**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-271-01

13. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.354715
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.424589
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.431629

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.436421

14. **SUSE**

https://www.suse.com/support/update/announcement/2017/suse-su-20172552-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172555-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172569-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172570-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172589-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172590-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172591-1/

15. **Trend Micro OfficeScan**

https://success.trendmicro.com/solution/1118372

16. **Ubuntu**

https://usn.ubuntu.com/usn/usn-3429-1/

17. **Xen**

http://xenbits.xen.org/xsa/advisory-245.html

Sources of product vulnerability information:

Apple
Cisco
CentOS
Debian
F5
Gentoo Linux
HKCERT
IBM
ICS-CERT
Mozilla Firefox
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
Xen

Contacts:

cert@govcert.gov.hk