GovCERT.HK

Weekly IT Security News Bulletin, 2017-W15

10 April – 16 April 2017

Headlines

Stealing PINs via mobile sensors: actual risk versus user perception

- Cyber security researchers at Newcastle University, United Kingdom, have presented a JavaScript-based side channel attack on an Android mobile phone. A JavaScript code embedded in a web page visited by a user collects the motion and orientation sensor streams of the phone; for example, the way the user clicks, scrolls, holds and taps the phone results in some recognizable tilt patterns. The streams are analysed using an artificial neural network to infer the user PIN, with a success rate of 94% within three attempts on a test set of 50 4-digit PINs.

- The study also included surveys on how mobile phone users perceive the risks associated with the sensors and found that there is a significant disparity between the actual and perceived levels of threat of compromising user PINs. People are far more concerned about security risks from camera and GPS than dozens of other sensors widely adopted by most mobile devices, such as the gyroscope, proximity, NFC, rotation sensors and accelerometer, which can usually be accessed by apps without seeking user permissions.

- The research team has alerted major mobile browser vendors, including Google, Apple, Mozilla and Firefox, some of which have partially fixed the issue but the ultimate solution is not available.

Advice

- Change PINs and passwords frequently to make pattern recognition difficult.

- Keep mobile device operating system and apps up-to-date and avoid using de-supported devices.

- Download and install apps only from official sources.

- Review permissions requested before installing apps.

- Close apps at the background when not in use and uninstall unnecessary apps.

Sources

- International Journal of Information Security
- Newcastle University
- Softpedia

Shadow Brokers release more NSA exploits

- On the 8th and 14th of April 2017, a hacker group named "Shadow Brokers", released the hacking tools alleged used by the U.S. National Security Agency (NSA) associated threat actor "Equation Group".

- The released hacking tools include exploits targeting Windows PCs and servers, Solaris and Cisco firewalls, Linux keyloggers, cross-platform remote access Trojan (RAT), system fingerprinting tools, and Apache and Samba zero-day exploits affecting several Linux distributions.

- The disclosed contents include a list of domains and IP addresses that were thought to be targeted by the Equation Group. There are no ".hk" domains observed.

Advice

- Always apply the latest security patches recommended by product vendors as soon as possible to avoid being exploited through known product vulnerabilities.

- Deploy intrusion detection systems and procedures to monitor and review network and system activities against potential intrusions.

- Establish and regularly drill the information security incident handling procedures for effective and prompt response when any intrusions are identified.

Sources

- Security Week
- Medium
- ZDNet
- Targeted List of Domains and IPs

何郭佩珍中學電郵泄學生及家長資料

- 孔教學院大成何郭佩珍中學校長於 2017 年 4 月 11 日向家長及學生發通告指校方於 4 月 9 日誤將多名學生個人資料，包括學生姓名、出生年份、身分證首 4 位數字、個人電話號碼、緊急聯絡人姓名及其電話號碼等，以電郵向全體學生發布。

- 有關通告指，事緣負責活動「背包跑」聯絡的老師在活動舉行前透過學校內聯網以電郵發放「備忘錄」提醒同學當天的注意事項，但不慎誤把學生個人資料一併發送，而外泄的資料並未作加密處理。

- 校方已啟動危機處理小組跟進，包括要求學校內聯網網絡供應商刪除有關電郵、向私隱專員公署陳述情況及徵詢意見、提醒同學刪除及不要下載和轉寄相關電郵、聯絡受影響的學生和家長留意不明來電、以及向教育局和校董會匯報事件。校方強調日後處理私隱資料時會提高警覺性。

Advice

- 處理個人資料時須遵守《個人資料（私隱）條例》（第 486 章）的規定，特別是保障資料第 4 原則 — 個人資料的保安。資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

- 在發送電郵前，應檢視及確保電郵只會傳送至指定收件人。如需以電郵傳送載有個人及敏感資料，應確保該等資料已被加密。

- 定期檢討處理個人及敏感資料的程序和執行安排，並提醒員工處理個人資料時務須提高警惕。

Sources

- 明報
- 星島日報
- 東網
- 個人資料私隱專員公署

Product Vulnerability Notes & Security Updates

1. **Adobe Flash Player and Adobe Reader/Acrobat**
   https://helpx.adobe.com/security/products/acrobat/apsb17-11.html
   https://helpx.adobe.com/security/products/flash-player/apsb17-10.html

2. **Apache Tomcat**
   http://tomcat.apache.org/security-7.html
   http://tomcat.apache.org/security-8.html
   http://tomcat.apache.org/security-9.html

3. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-April/022355.html
   https://lists.centos.org/pipermail/centos-announce/2017-April/022358.html

4. **DBPOWER U818A WIFI quadcopter drone**
   http://www.kb.cert.org/vuls/id/334207

5. **Debian**
   https://www.debian.org/security/2017/dsa-3827
   https://www.debian.org/security/2017/dsa-3828
   https://www.debian.org/security/2017/dsa-3829

6. **F5 Products**
   https://support.f5.com/csp/article/K53244431
   https://support.f5.com/csp/article/K90879323
   https://support.f5.com/csp/article/K34527393
   https://support.f5.com/csp/article/K44503763
   https://support.f5.com/csp/article/K52828640

7. **FreeBSD**
   https://security.freebsd.org/advisories/FreeBSD-SA-17:03.ntp.asc

8. **Gentoo Linux**
   https://security.gentoo.org/glsa/201704-01
   https://security.gentoo.org/glsa/201704-02
   https://security.gentoo.org/glsa/201704-03

9. **IBM InfoSphere Information Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg21991682
   http://www-01.ibm.com/support/docview.wss?uid=swg21995155

10. **ISC BIND**
    https://kb.isc.org/article/AA-01465/
    https://kb.isc.org/article/AA-01466/
    https://kb.isc.org/article/AA-01471/

11. **Microsoft Products**
    https://www.hkcert.org/my_url/en/alert/17041101
    http://www.kb.cert.org/vuls/id/921560
    https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/42b8fa28-9d09-e711-80d9-000d3a32fc99

https://portal.msrc.microsoft.com/en-us/security-guidance

12. **OpenSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00011.html
    https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00012.html

13. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-0892.html
    https://linux.oracle.com/errata/ELSA-2017-0893.html
    https://linux.oracle.com/errata/ELSA-2017-0906.html
    https://linux.oracle.com/errata/ELSA-2017-0907.html
    https://linux.oracle.com/errata/ELSA-2017-0914.html
    https://linux.oracle.com/errata/ELSA-2017-0920.html
    https://linux.oracle.com/errata/ELSA-2017-0933.html
    https://linux.oracle.com/errata/ELSA-2017-0935.html

14. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:0906
    https://access.redhat.com/errata/RHSA-2017:0907
    https://access.redhat.com/errata/RHSA-2017:0914
    https://access.redhat.com/errata/RHSA-2017:0920
    https://access.redhat.com/errata/RHSA-2017:0931
    https://access.redhat.com/errata/RHSA-2017:0932
    https://access.redhat.com/errata/RHSA-2017:0933
    https://access.redhat.com/errata/RHSA-2017:0934
    https://access.redhat.com/errata/RHSA-2017:0935
    https://access.redhat.com/errata/RHSA-2017:0936
    https://access.redhat.com/errata/RHSA-2017:0937
    https://access.redhat.com/errata/RHSA-2017:0938
    https://access.redhat.com/errata/RHSA-2017:0898

15. **Schneider Electric Modicon Modbus Protocol**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-101-01

16. **Splunk Enterprise**
    http://www.splunk.com/view/SP-CAAAPZ3

17. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.395195
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.403724

18. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170962-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170966-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170967-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170983-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170990-1.html

19. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3257-1/
    https://www.ubuntu.com/usn/usn-3258-1/

https://www.ubuntu.com/usn/usn-3258-2/

Sources of product vulnerability information:

Adobe
Apache Tomcat
CERT/CC
CentOS
Debian
F5
FreeBSD
Gentoo Linux
HKCERT
IBM
ICS-CERT
ISC BIND
Microsoft
openSUSE
Oracle Linux
Red Hat
Splunk
Slackware
SUSE
Ubuntu
US-CERT

Contacts:

cert@govcert.gov.hk