GovCERT.HK

Weekly IT Security News Bulletin, 2017-W29

17 July – 23 July 2017

Headlines

A "key" milestone in protecting the DNS

- On 11 July 2017, the Internet Corporation for Assigned Names and Numbers (ICANN) published the new Domain Name System Security Extensions (DNSSEC) Key Signing Key (KSK-2017) in the DNS root zone, as a step forward to prepare for the first ever Root Zone KSK Rollover on 11 October 2017.

- The Rollover operations began on 27 October 2016 when the new cryptographic public/private key pair, i.e. KSK-2017, was made during the Root KSK Ceremony at ICANN's secure key management facility in Culpeper, Virginia. The new key will replace the first and currently functional root zone KSK used since 2010 (KSK-2010) on and after the Rollover date. Then every Internet query using DNSSEC query will depend on the new key to validate the destination.

- Operators of DNSSEC recursive servers need to update their systems with the new key before the Rollover; otherwise, end users relying on those resolvers will encounter errors and be unable to access the Internet. For DNSSEC systems supporting the RFC 5011 automated KSK updates, ICANN offers a test bed (https://go.icann.org/KSKtest) for operators to verify if their systems handle the automated update process correctly.

Advice

- The change should be transparent to most end users as DNSSEC validation is usually performed by the Internet service providers. Users may approach their service provider(s) if they wish to know whether DNSSEC is enabled for their Internet access service.

- Operators of DNSSEC recursive servers should review their system configurations to ensure timely key updates either automatically or manually. For systems supporting IETF RFC 5011, the automatic update function should be enabled and verified using the test bed provided by ICANN.

- The latest status and events of the Rollover operations by ICANN should be closely monitored for better preparation of the change.

Sources

- ICANN
- North American Network Operators' Group (NANOG)

消委會：通訊 App 欠點對點加密　訊息易外泄

- 消費者委員會（消委會）於最新出版的《選擇》月刊 489 期發表測試報告，指出 6 款流動即時通訊應用程式包括 Google Hangouts、微信 WeChat、Skype、imo、Snapchat 及 Instagram，傳送信息時未有使用點對點加密（end-to-end encryption）技術，來避免傳送和接收訊息者以外第三方讀取訊息內容，或未能有效保護數據在傳送時的安全性。

- 在登入帳戶的保安方面，除了 WhatsApp、Viber、Google Allo 及 imo 以外，其餘都設有登入帳戶或個人識別號碼，而 LINE 更同時設有登入帳戶及個人識別碼，保障用戶方面評分較高。而在個人資料保障方面，微信 WeChat 的 Android 版本會把用戶的個人資料傳送至廠方伺服器，而且沒有將資料加密。另外，Apple iMessage 在用戶使用前，並沒有說明其私隱政策，用戶個人資料保障度存疑。

- 是次測試由歐洲消費者組織（Euro consumers）統籌，委託一所歐洲實驗室於 2017 年 1 月至 3 月測試了合共 13 款 Android 及 iOS 系統的 25 個版本即時通訊應用程式，就其功能安全性、多元性、使用方便程度評分，並檢視這些應用程式會否有機會將手機內的敏感資料外泄。

Advice

- 不要在通訊應用程式上傳送任何敏感或保密資料，以免資料被盜。

- 在安裝任何流動應用程式之前，用戶須細閱其所要求存取的權限，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。

- 用戶應留意私隱政策及使用條款之變更，如程式設有內置加密及雙重認證等保安功能，用戶應及早啟動。

Sources

- 消費者委員會
- 東網
- 香港經濟日報

Product Vulnerability Notes & Security Updates

1. **Apache Struts**
   https://struts.apache.org/docs/s2-049.html

2. **Apple iOS, MacOS, iTunes for Windows, Safari and iCloud**
   https://support.apple.com/kb/HT207921
   https://support.apple.com/kb/HT207922
   https://support.apple.com/kb/HT207923
   https://support.apple.com/kb/HT207927
   https://support.apple.com/kb/HT207928

3. **CentOS**
   https://lists.centos.org/pipermail/centos-announce-July/022507.html

4. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-asr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-asr1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-pcpt
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa5

5. **Cisco WebEx Browser Extension**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170717-webex
   https://www.hkcert.org/my_url/en/alert/17071801

6. **Debian**
   https://www.debian.org/security/2017/dsa-3909
   https://www.debian.org/security/2017/dsa-3910
   https://www.debian.org/security/2017/dsa-3911
   https://www.debian.org/security/2017/dsa-3912
   https://www.debian.org/security/2017/dsa-3913
   https://www.debian.org/security/2017/dsa-3914
   https://www.debian.org/security/2017/dsa-3915

7. **F5 Products**
   https://support.f5.com/csp/article/K05415626
   https://support.f5.com/csp/article/K15004519
   https://support.f5.com/csp/article/K45439210
   https://support.f5.com/csp/article/K54170502
   https://support.f5.com/csp/article/K75429050

8. **Huawei Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170720-01-ospf-en

9. **IBM InfoSphere Information Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg21982420

10. **IBM WebSphere Application Server**
    http://www-01.ibm.com/support/docview.wss?uid=swg22004785

http://www-01.ibm.com/support/docview.wss?uid=swg22004786
http://www-01.ibm.com/support/docview.wss?uid=swg22004792

11. **IBM HTTP Server**
    http://www-01.ibm.com/support/docview.wss?uid=swg22005280

12. **Juniper Products**
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10775
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10779
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10787
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10789
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10792
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10793
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10803
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10804
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10805
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10806
    https://www.hkcert.org/my_url/en/alert/17071401

13. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00023.html
    https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00024.html
    https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00025.html

14. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-1759.html
    https://linux.oracle.com/errata/ELSA-2017-1789.html
    https://linux.oracle.com/errata/ELSA-2017-1793.html

15. **Oracle Products**
    http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html

16. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:1759
    https://access.redhat.com/errata/RHSA-2017:1766
    https://access.redhat.com/errata/RHSA-2017:1787
    https://access.redhat.com/errata/RHSA-2017:1789
    https://access.redhat.com/errata/RHSA-2017:1790
    https://access.redhat.com/errata/RHSA-2017:1791
    https://access.redhat.com/errata/RHSA-2017:1792
    https://access.redhat.com/errata/RHSA-2017:1793

17. **Rockwell Automation MicroLogix 1100 Controllers**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-138-03

18. **Schneider Electric PowerSCADA Anywhere and Citect Anywhere**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-201-01

19. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.377075
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.405076

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.458982
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.536169

20. SUSE

https://www.suse.com/support/update/announcement/2017/suse-su-20171859-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171860-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171861-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171862-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171865-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171866-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171868-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171886-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171893-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171894-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171898-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171901-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171903-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171904-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171905-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171906-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171907-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171908-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171909-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171910-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171911-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171912-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171913-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171914-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171915-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171916-1.html

21. Ubuntu

https://usn.ubuntu.com/usn/usn-3212-3/
https://usn.ubuntu.com/usn/usn-3274-2/
https://usn.ubuntu.com/usn/usn-3307-2/
https://usn.ubuntu.com/usn/usn-3309-2/
https://usn.ubuntu.com/usn/usn-3347-2/
https://usn.ubuntu.com/usn/usn-3353-1/
https://usn.ubuntu.com/usn/usn-3353-2/
https://usn.ubuntu.com/usn/usn-3354-1/
https://usn.ubuntu.com/usn/usn-3355-1/
https://usn.ubuntu.com/usn/usn-3356-1/
https://usn.ubuntu.com/usn/usn-3356-2/
https://usn.ubuntu.com/usn/usn-3357-1/
https://usn.ubuntu.com/usn/usn-3358-1/

Sources of product vulnerability information:

- Apache Struts
- Apple
- CentOS
- Cisco
- Debian
- F5
- Huawei
- HKCERT
- IBM
- ICS-CERT
- Juniper
- Mageia
- openSUSE
- Oracle
- Oracle Linux
- Red Hat
- Slackware
- SUSE
- Ubuntu

Contacts:

cert@govcert.gov.hk