GovCERT.HK

Weekly IT Security News Bulletin, 2017-W2
9 January – 15 January 2017

Headlines

Keynote Speech by Mr. Victor Lam, JP, Deputy Government Chief Information Officer, at the "Gazing Through the Crystal Ball: Cyber-Security 2017 - Predicting the Good, the Bad and the Ugly" Seminar

- To make Hong Kong digitally safe, cooperation between the Government, academia, industry, professional bodies and general public is a must. The Government Computer Emergency Response Team Hong Kong was established to coordinate the work in response to information and cyber security incidents for the Government and collaborate with other CERTs worldwide. SMEs and the general public were reached for awareness education by public seminars, school visits, broadcasting media, social media and thematic websites.

- The review of Government IT Security Policy and Guidelines was highlighted, including the alignment with the ISO 27001 and ISO 27002 international information security standards and enrichment of the library of practice guides for practical security implementation references.

- For governance, the central Information Security Management Committee oversees the government-wide IT security while bureaux/departments have individual security management structures with clearly defined roles and responsibilities and strong leadership of senior officials.

Advice

- Government users should follow the government security requirements to protect government information systems and assets against emerging security threats.

- All cyber citizens should stay vigilant against cyber attacks all times and could frequently visit the Cyber Security Information Portal for practical tips, advice and useful tools.

- The Government, the academia, the private sector, international partners and individuals all have vital roles to play. We must join hands to enhance capabilities to safeguard against cyber security threats.

Sources

- OGCIO Homepage
- GovCERT.HK Homepage

MongoDB ransomware attack

- MongoDB was regarded as the most popular NoSQL database management system at the moment. More than 28,000 Internet-facing MongoDB database servers were suffered with a new wave of ransomware attack, where no malware and phishing were required.

- The attackers scanned for installations lacking a set administrator password, took over the administrator account and moved away the data, just leaving a ransom demand note. The database and system administrators did not follow the basic security practices, architectural design and access control, such as zones separating the database, application and web servers for multi-layer protection.

- There was unknown impact to the affected organisations. If regular backup is taken, the data could still be restored without paying the ransom. But attackers could also analyse individual businesses before encrypting those valuable data. The trend may be turning from high-volume attacks to low-volume attacks with higher ransom amounts.

Advice

- System and database administrator should adopt multiple layers of defences against direct access to the data through the Internet.

- A third-party security risk assessment with vulnerability scanning and penetration testing are recommended for Internet-facing systems holding important data.

- Monitoring of suspicious activities such as scanning and unauthorised access should be carried out to get advanced information of intrusion threats

Sources

- nixCraft
- Krebs on Security
- Victor Gevers Tweet
- Niall Merrigan Tweet

Product Vulnerability Notes & Security Updates

1. **Advantech WebAccess**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-012-01

2. **Adobe Flash Player and Adobe Reader/Acrobat**
   https://helpx.adobe.com/security/products/acrobat/apsb17-01.html
   https://helpx.adobe.com/security/products/flash-player/apsb17-02.html

3. **Carlo Gavazzi**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-012-03

4. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-January/022194.html
   https://lists.centos.org/pipermail/centos-announce/2017-January/022195.html
   https://lists.centos.org/pipermail/centos-announce/2017-January/022196.html
   https://lists.centos.org/pipermail/centos-announce/2017-January/022197.html
   https://lists.centos.org/pipermail/centos-announce/2017-January/022206.html
   https://lists.centos.org/pipermail/centos-announce/2017-January/022207.html
   https://lists.centos.org/pipermail/centos-announce/2017-January/022209.html
   https://lists.centos.org/pipermail/centos-announce/2017-January/022210.html

5. **Debian**
   https://www.debian.org/security/2017/dsa-3752
   https://www.debian.org/security/2017/dsa-3754
   https://www.debian.org/security/2017/dsa-3755
   https://www.debian.org/security/2017/dsa-3756
   https://www.debian.org/security/2017/dsa-3757
   https://www.debian.org/security/2017/dsa-3759
   https://www.debian.org/security/2017/dsa-3760

6. **F5 Products**
   https://support.f5.com/csp/#/article/K97285349

7. **FreeBSD**
   https://security.freebsd.org/advisories/FreeBSD-SA-17:01.openssh.asc

8. **Huawei Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170111-01-parser-en

9. **IBM Products**
   http://www-01.ibm.com/support/docview.wss?uid=swg21995155
   http://www-01.ibm.com/support/docview.wss?uid=swg21995257

10. **ISC BIND**
    https://kb.isc.org/article/AA-01439
    https://kb.isc.org/article/AA-01440
    https://kb.isc.org/article/AA-01441
    https://kb.isc.org/article/AA-01442

11. **Gentoo Linux**
    https://security.gentoo.org/glsa/201701-16
    https://security.gentoo.org/glsa/201701-17

https://security.gentoo.org/glsa/201701-18
https://security.gentoo.org/glsa/201701-19
https://security.gentoo.org/glsa/201701-20
https://security.gentoo.org/glsa/201701-21
https://security.gentoo.org/glsa/201701-22
https://security.gentoo.org/glsa/201701-23
https://security.gentoo.org/glsa/201701-24
https://security.gentoo.org/glsa/201701-25
https://security.gentoo.org/glsa/201701-26
https://security.gentoo.org/glsa/201701-27
https://security.gentoo.org/glsa/201701-28
https://security.gentoo.org/glsa/201701-29
https://security.gentoo.org/glsa/201701-30
https://security.gentoo.org/glsa/201701-31
https://security.gentoo.org/glsa/201701-32
https://security.gentoo.org/glsa/201701-33
https://security.gentoo.org/glsa/201701-34

12. **Mageia**

http://advisories.mageia.org/MGASA-2017-0005.html
http://advisories.mageia.org/MGASA-2017-0006.html
http://advisories.mageia.org/MGASA-2017-0007.html
http://advisories.mageia.org/MGASA-2017-0008.html
http://advisories.mageia.org/MGASA-2017-0009.html
http://advisories.mageia.org/MGASA-2017-0010.html
http://advisories.mageia.org/MGASA-2017-0011.html
http://advisories.mageia.org/MGASA-2017-0012.html
http://advisories.mageia.org/MGASA-2017-0013.html

13. **Microsoft Products**

https://technet.microsoft.com/en-us/library/security/ms17-jan
https://technet.microsoft.com/en-us/library/security/MS17-001
https://technet.microsoft.com/en-us/library/security/MS17-002
https://technet.microsoft.com/en-us/library/security/MS17-003
https://technet.microsoft.com/en-us/library/security/MS17-004

14. **openSUSE**

https://lists.opensuse.org/opensuse-security-announce/2017-01/msg00007.html
https://lists.opensuse.org/opensuse-security-announce/2017-01/msg00009.html
https://lists.opensuse.org/opensuse-security-announce/2017-01/msg00012.html

15. **Oracle Linux**

https://linux.oracle.com/errata/ELSA-2017-0036.html
https://linux.oracle.com/errata/ELSA-2017-0061.html
https://linux.oracle.com/errata/ELSA-2017-3508.html
https://linux.oracle.com/errata/ELSA-2017-3509.html
https://linux.oracle.com/errata/ELSA-2017-3510.html

16. **Red Hat**

https://access.redhat.com/errata/RHSA-2017:0031
https://access.redhat.com/errata/RHSA-2017:0036
https://access.redhat.com/errata/RHSA-2017:0057
https://access.redhat.com/errata/RHSA-2017:0059

https://access.redhat.com/errata/RHSA-2017:0061

17. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.440416
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.551910
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.602456

18. **St. Jude Medical's Merlin@home Transmitter**
    https://ics-cert.us-cert.gov/advisories/ICSMA-17-009-01

19. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170084-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170102-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170103-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170104-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170108-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170109-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170110-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170111-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170112-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170113-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170114-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170116-1.html

20. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3166-1/
    https://www.ubuntu.com/usn/usn-3167-1/
    https://www.ubuntu.com/usn/usn-3167-2/
    https://www.ubuntu.com/usn/usn-3168-1/
    https://www.ubuntu.com/usn/usn-3168-2/
    https://www.ubuntu.com/usn/usn-3169-1/
    https://www.ubuntu.com/usn/usn-3169-2/
    https://www.ubuntu.com/usn/usn-3169-3/
    https://www.ubuntu.com/usn/usn-3169-4/
    https://www.ubuntu.com/usn/usn-3170-1/
    https://www.ubuntu.com/usn/usn-3170-2/
    https://www.ubuntu.com/usn/usn-3171-1/
    https://www.ubuntu.com/usn/usn-3172-1

21. **VideoInsight Web Client**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-012-02

22. **WordPress**
    https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/

Sources of product vulnerability information:

- CentOS
- Debian
- F5
- FreeBSD
- Gentoo
- Huawei
- IBM
- ISC
- ICS-CERT
- Mageia
- openSUSE
- Oracle Linux
- Red Hat
- Slackware
- SUSE
- Ubuntu
- WordPress

Contacts:

cert@govcert.gov.hk