GovCERT.HK

Weekly IT Security News Bulletin, 2017-W25

19 June – 25 June 2017

Headlines

The British Parliament has been hit by a cyberattack

- The British Parliament suffered from a cyber attack on 23 June 2017 morning. Attackers launched sustained and determined attempts to identify weak passwords of all parliamentary user email accounts.

- In response to the attack, the official stopped the remote access of email service for Members of Parliament and their staff via mobiles and computers outside of the official buildings to prevent the attackers from breaking their way into the system. A spokesman said the attack was a result of weak passwords and some 90 email accounts were compromised, fewer than 1% of the 9,000 users of the IT system. The authority was working closely with the National Cyber Security Centre (NCSC) of United Kingdom to identify the method of the attack and take further measures to secure the computer network where necessary.

- Security experts also warned that politicians could be exposed to blackmail or face a heightened threat of terrorist attack if emails were successfully accessed.

Advice

- Use strong passwords to protect your information asset and change your passwords regularly.

- Stay vigilant on suspicious activities and alerts prompted from your systems.

- Apply account lock out features and maintain log records for all logon and logout activities.

- Always have an incident response and business continuity plan to cater for cyber attacks and service interruption or termination.

Sources

- BBC News: 24 June, 26 June
- HuffPost UK
- The Telegraph
- NCSC

Few victims reporting ransomware attacks to FBI

- Ransomware have been the prevalent cyber threat against every Internet users and organisations in the past year. According to the 2016 annual report published by the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3) last week, ransomware, business e-mail compromise scam, tech support fraud and extortion are the hottest topics in 2016.

- In September 2016, the FBI urged victims to report ransomware incidents to federal law enforcement regardless of whether or not they paid the demanded ransom. By reporting the case to the law enforcement, it helps the FBI with a greater understanding of the threat and determine who is behind the attacks and how they are identifying or targeting the victims. However, according to the U.S. Boston Police Department, victims mostly do not willing to report to the police because the report will become a public record.

- New ransomware variants are emerging quickly. Collaboration and timely sharing of information is important when it comes to fighting ransomware and other cyber attacks.

Advice

- Share threat intelligence timely with trusted partners, such as computer emergency response teams (CERTs) and law enforcement agency.

- Report to the Hong Kong Police Force for any technology crime cases to facilitate the investigation.

- Apply security patches of computer devices and keep the anti-malware solution and signatures up-to-date to defend against ransomware.

Sources

- 2016 Internet Crime Report
- FBI Public Service Announcement
- Threatpost

Personal details of nearly 200 million U.S. citizens exposed

- Near 200 million U.S. electors' personal information stored in spreadsheets were found exposing to the Internet on 12 June 2017. UpGuard, a security company, discovered that 1.1 terabytes of data was publicly accessible on an Amazon cloud server which was owned by Deep Root Analytics, a Republican data firm working for the Republican National Committee. The data included birth dates, home addresses, telephone numbers and political views.

- From UpGuard's report, the data found in the Amazon server was not secured by any protection measures against unauthorised access. The misconfiguration in the cloud server was the root cause of this data leakage incident. Anyone who typed in a six-character Amazon subdomain:"dra-dw", could retrieve the electors' personal information, where this subdomain can be easily discovered through a random generator.

Advice

- Avoid deploying default settings on servers. Configure the server with secure settings properly, such as enabling the access control and logging.

- Conduct security risk assessment and vulnerability scanning periodically to uncover any misconfigurations.

- Require the same level of security protection measures have been applied by your outsourced services contractors.

- Raise the awareness of all employees by providing regular training programs on how to handle personal and sensitive information securely.

Sources

- UpGuard
- BBC News
- Wired
- The Guardian

Product Vulnerability Notes & Security Updates

1. **Apache HTTP Server**
   https://httpd.apache.org/security/vulnerabilities_22.html#2.2.33-dev
   https://httpd.apache.org/security/vulnerabilities_24.html#2.4.26

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-June/022461.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022462.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022463.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022464.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022467.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022468.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022469.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022470.html

3. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-asr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-csm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-fmc1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-fmc2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-fpmc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-ios
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-ios1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-ise
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-ise1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-pcp1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-pcp2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-pcp3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-pcp4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piepnm1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piepnm2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piepnm3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piepnm4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piwf
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piwf1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-ucce
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-vpc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-waas
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-wnrp

4. **Debian**
   https://www.debian.org/security/2017/dsa-3884
   https://www.debian.org/security/2017/dsa-3885
   https://www.debian.org/security/2017/dsa-3886
   https://www.debian.org/security/2017/dsa-3887
   https://www.debian.org/security/2017/dsa-3888
   https://www.debian.org/security/2017/dsa-3889

https://www.debian.org/security/2017/dsa-3890
https://www.debian.org/security/2017/dsa-3891
https://www.debian.org/security/2017/dsa-3892
https://www.debian.org/security/2017/dsa-3893
https://www.debian.org/security/2017/dsa-3894
https://www.debian.org/security/2017/dsa-3895
https://www.debian.org/security/2017/dsa-3896

5. **Drupal**
   https://www.drupal.org/SA-CORE-2017-003

6. **Ecava IntegraXor**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-171-01

7. **EMC Avamar Server**
   https://exchange.xforce.ibmcloud.com/vulnerabilities/127414
   https://exchange.xforce.ibmcloud.com/vulnerabilities/127415

8. **EMC Isilon OneFS**
   https://exchange.xforce.ibmcloud.com/vulnerabilities/127413

9. **EMC VNX1 and VNX2**
   https://exchange.xforce.ibmcloud.com/vulnerabilities/127351
   https://exchange.xforce.ibmcloud.com/vulnerabilities/127352
   https://exchange.xforce.ibmcloud.com/vulnerabilities/127353

10. **F5 Products**
    https://support.f5.com/csp/article/K31603170

11. **FortiOS**
    http://fortiguard.com/psirt/FG-IR-17-127

12. **Gentoo Linux**
    https://security.gentoo.org/glsa/201706-16
    https://security.gentoo.org/glsa/201706-17
    https://security.gentoo.org/glsa/201706-18
    https://security.gentoo.org/glsa/201706-19
    https://security.gentoo.org/glsa/201706-20
    https://security.gentoo.org/glsa/201706-21
    https://security.gentoo.org/glsa/201706-22
    https://security.gentoo.org/glsa/201706-23
    https://security.gentoo.org/glsa/201706-24
    https://security.gentoo.org/glsa/201706-25
    https://security.gentoo.org/glsa/201706-26

13. **IBM InfoSphere Information Server**
    http://www-01.ibm.com/support/docview.wss?uid=swg21995427

14. **libcurl**
    https://curl.haxx.se/docs/adv_20170614.html
    https://www.hkcert.org/my_url/en/alert/17061602

15. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0178.html
    http://advisories.mageia.org/MGASA-2017-0179.html
    http://advisories.mageia.org/MGASA-2017-0180.html

16. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00017.html
    https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00020.html
    https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00024.html
    https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00026.html

17. **OpenVPN**
    https://community.openvpn.net/openvpn/wiki/VulnerabilitiesFixedInOpenVPN243
    https://www.hkcert.org/my_url/en/alert/17062301

18. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-1480.html
    https://linux.oracle.com/errata/ELSA-2017-1481.html
    https://linux.oracle.com/errata/ELSA-2017-1484-1.html
    https://linux.oracle.com/errata/ELSA-2017-1484.html
    https://linux.oracle.com/errata/ELSA-2017-1486.html
    https://linux.oracle.com/errata/ELSA-2017-1574.html
    https://linux.oracle.com/errata/ELSA-2017-3582.html
    https://linux.oracle.com/errata/ELSA-2017-3583.html

19. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:1479
    https://access.redhat.com/errata/RHSA-2017:1480
    https://access.redhat.com/errata/RHSA-2017:1481
    https://access.redhat.com/errata/RHSA-2017:1482
    https://access.redhat.com/errata/RHSA-2017:1483
    https://access.redhat.com/errata/RHSA-2017:1484
    https://access.redhat.com/errata/RHSA-2017:1485
    https://access.redhat.com/errata/RHSA-2017:1486
    https://access.redhat.com/errata/RHSA-2017:1487
    https://access.redhat.com/errata/RHSA-2017:1488
    https://access.redhat.com/errata/RHSA-2017:1489
    https://access.redhat.com/errata/RHSA-2017:1490
    https://access.redhat.com/errata/RHSA-2017:1491
    https://access.redhat.com/errata/RHSA-2017:1495
    https://access.redhat.com/errata/RHSA-2017:1499
    https://access.redhat.com/errata/RHSA-2017:1504
    https://access.redhat.com/errata/RHSA-2017:1508
    https://access.redhat.com/errata/RHSA-2017:1537
    https://access.redhat.com/errata/RHSA-2017:1546
    https://access.redhat.com/errata/RHSA-2017:1548
    https://access.redhat.com/errata/RHSA-2017:1549
    https://access.redhat.com/errata/RHSA-2017:1550
    https://access.redhat.com/errata/RHSA-2017:1552
    https://access.redhat.com/errata/RHSA-2017:1558
    https://access.redhat.com/errata/RHSA-2017:1567
    https://access.redhat.com/errata/RHSA-2017:1574

20. **SIMATIC CP 44x-1 Redundant Network Access modules**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-173-01

21. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.569890

22. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20171576-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171577-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171581-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171582-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171585-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171587-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171599-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171600-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171603-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171606-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171608-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171611-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171613-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171614-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171615-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171617-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171618-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171619-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171621-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171622-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171626-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171627-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171628-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171632-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171635-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171642-1.html

23. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3311-2/
    https://www.ubuntu.com/usn/usn-3322-1/
    https://www.ubuntu.com/usn/usn-3323-1/
    https://www.ubuntu.com/usn/usn-3324-1/
    https://www.ubuntu.com/usn/usn-3324-1/
    https://www.ubuntu.com/usn/usn-3325-1/
    https://www.ubuntu.com/usn/usn-3325-1/
    https://www.ubuntu.com/usn/usn-3326-1/
    https://www.ubuntu.com/usn/usn-3327-1/
    https://www.ubuntu.com/usn/usn-3328-1/
    https://www.ubuntu.com/usn/usn-3329-1/
    https://www.ubuntu.com/usn/usn-3330-1/
    https://www.ubuntu.com/usn/usn-3331-1/
    https://www.ubuntu.com/usn/usn-3332-1/
    https://www.ubuntu.com/usn/usn-3333-1/
    https://www.ubuntu.com/usn/usn-3334-1/
    https://www.ubuntu.com/usn/usn-3335-1/

https://www.ubuntu.com/usn/usn-3335-2/
https://www.ubuntu.com/usn/usn-3336-1/
https://www.ubuntu.com/usn/usn-3337-1/
https://www.ubuntu.com/usn/usn-3338-1/
https://www.ubuntu.com/usn/usn-3339-1/

24. Xen

http://xenbits.xen.org/xsa/advisory-216.html
http://xenbits.xen.org/xsa/advisory-217.html
http://xenbits.xen.org/xsa/advisory-218.html
http://xenbits.xen.org/xsa/advisory-219.html
http://xenbits.xen.org/xsa/advisory-220.html
http://xenbits.xen.org/xsa/advisory-221.html
http://xenbits.xen.org/xsa/advisory-222.html
http://xenbits.xen.org/xsa/advisory-223.html
http://xenbits.xen.org/xsa/advisory-224.html
http://xenbits.xen.org/xsa/advisory-225.html

Sources of product vulnerability information:

Apache
CentOS
Cisco
Debian
Drupal
F5
FortiGuard
Gentoo Linux
HKCERT
IBM
IBM X-Force Exchange
ICS-CERT
libcurl
Mageia
openSUSE
OpenVPN
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
Xen

Contacts:

cert@govcert.gov.hk