GovCERT.HK

Weekly IT Security News Bulletin, 2017-W13

27 March– 2 April 2017

Headlines

Suspected theft of Registration and Electoral Office computers

- On 27 March 2017, the Registration and Electoral Office (REO) issued a press release reporting that two government notebook computers stored at the fallback venue of the 2017 Chief Executive Election were suspected to be stolen from a locked room at the AsiaWorld-Expo with closed-circuit televisions.

- One computer contains the names of Election Committee members with no other personal information. The other computer contains the names, addresses and Hong Kong Identity Card numbers of electors of geographical constituency which have been encrypted in accordance with the relevant security requirements. No voting records are stored on these notebook computers.

- REO has issued a letter to all affected electors of geographical constituencies by email or by post to notify them of the earlier suspected theft of notebook computers containing voter registration particulars to increase their awareness and mitigate potential damage.

Advice

- Assess business needs and associated risk to store classified information on portable devices such as laptops, mobile phones, etc.

- Avoid storing classified information on portable devices unless otherwise deemed necessary for operational needs. In case of necessity, there should be proper authorisation and B/Ds shall comply with the Security Regulations in relation to the information classification, labelling and handling.

- Always use mobile devices and removable media provided by the B/D, encrypt classified information and remove it according to proper procedure immediately after use.

Sources

- Registration and Electoral Office: 27 Mar, 28 Mar, 30 Mar
- Constitutional and Mainland Affairs Bureau: 27 Mar, 28 Mar
- Electoral Affairs Commission: 28 Mar
- news.gov.hk: 31 Mar
- Baseline IT Security Policy (S17)

Exploit code released for zero-day in Microsoft's IIS 6.0

- Security researchers uncovered a zero-day buffer overflow vulnerability (CVE-2017-7269) on Microsoft Internet Information Services (IIS) 6.0 which could lead to remote code execution and denial of service conditions. A remote attacker could exploit this vulnerability in the IIS WebDAV Component with a specially crafted request using PROPFIND method. The U.S. National Vulnerability Database (NVD) assessed the vulnerability severity as "**Critical**" with the CVSS* v3 Base Score 9.8 out of the top severity score of 10.

- The researchers posted the exploit code on GitHub this week. Threat actors could make use of this exploit code to create new malicious code for attacks.

- Extended support for IIS 6.0, which was included with Windows Server 2003, has already ended in July 2015. It means that Microsoft will not provide security patch for this vulnerability. Newer versions of Windows Server installed with newer IIS versions are not vulnerable to the exploit.

Advice

- Stop using obsolete versions of Windows Server and IIS 6.0 and upgrade the software to the latest versions.

- Disable WebDAV, which is an HTTP protocol extension for remote web content authoring operations, if the service is not necessary.

- Ensure the signatures for web application firewalls, intrusion protection systems and other security protection devices are up-to-date to protect web systems against any newly disclosed vulnerabilities.

Sources

- GitHub
- NIST-NVD
- TrendMicro

*The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. Scores range from 0 to 10 with 10 being the most severe.

Product Vulnerability Notes & Security Updates

1. **3S-Smart Software Solutions GmbH CODESYS Web Server**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-087-02

2. **Apple products**
   https://support.apple.com/kb/HT207600
   https://support.apple.com/kb/HT207615
   https://support.apple.com/kb/HT207617
   https://support.apple.com/zh-hk/HT207607

3. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-March/022347.html
   https://lists.centos.org/pipermail/centos-announce/2017-March/022349.html

4. **Debian**
   https://www.debian.org/security/2017/dsa-3817
   https://www.debian.org/security/2017/dsa-3818
   https://www.debian.org/security/2017/dsa-3819
   https://www.debian.org/security/2017/dsa-3820
   https://www.debian.org/security/2017/dsa-3821
   https://www.debian.org/security/2017/dsa-3822
   https://www.debian.org/security/2017/dsa-3823
   https://www.debian.org/security/2017/dsa-3824

5. **F5 Products**
   https://support.f5.com/csp/article/K18015201

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201703-04
   https://security.gentoo.org/glsa/201703-05
   https://security.gentoo.org/glsa/201703-06
   https://security.gentoo.org/glsa/201703-07

7. **Google Chrome**
   https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop_29.html

8. **Huawei Video Content Management Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170329-01-vcm-en

9. **IBM Notes**
   http://www-01.ibm.com/support/docview.wss?uid=swg21990421
   http://www-01.ibm.com/support/docview.wss?uid=swg21990658

10. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0083.html
    http://advisories.mageia.org/MGASA-2017-0084.html
    http://advisories.mageia.org/MGASA-2017-0085.html
    http://advisories.mageia.org/MGASA-2017-0086.html
    http://advisories.mageia.org/MGASA-2017-0087.html
    http://advisories.mageia.org/MGASA-2017-0088.html
    http://advisories.mageia.org/MGASA-2017-0089.html

http://advisories.mageia.org/MGASA-2017-0090.html
http://advisories.mageia.org/MGASA-2017-0091.html
http://advisories.mageia.org/MGASA-2017-0092.html
http://advisories.mageia.org/MGASA-2017-0093.html
http://advisories.mageia.org/MGASA-2017-0094.html

11. NTP

http://support.ntp.org/bin/view/Main/SecurityNotice#March_2017_ntp_4_2_8p10_NTP_Secu
https://www.hkcert.org/my_url/en/alert/17032701

12. Oracle Linux

https://linux.oracle.com/errata/ELSA-2017-3531.html
https://linux.oracle.com/errata/ELSA-2017-0565.html
https://linux.oracle.com/errata/ELSA-2017-0725.html
https://linux.oracle.com/errata/ELSA-2017-0817.html
https://linux.oracle.com/errata/ELSA-2017-0680.html
https://linux.oracle.com/errata/ELSA-2017-0654.html
https://linux.oracle.com/errata/ELSA-2017-0631.html
https://linux.oracle.com/errata/ELSA-2017-0744.html
https://linux.oracle.com/errata/ELSA-2017-0794.html
https://linux.oracle.com/errata/ELSA-2017-0662.html
https://linux.oracle.com/errata/ELSA-2017-0564.html
https://linux.oracle.com/errata/ELSA-2017-0630.html
https://linux.oracle.com/errata/ELSA-2017-0621.html
https://linux.oracle.com/errata/ELSA-2017-0641.html
https://linux.oracle.com/errata/ELSA-2017-0574.html
https://linux.oracle.com/errata/ELSA-2017-0847.html

13. Samba

https://www.samba.org/samba/security/CVE-2017-2619.html
https://www.hkcert.org/my_url/en/alert/17032702

14. Schneider Electric Products

https://ics-cert.us-cert.gov/advisories/ICSA-17-089-01
https://ics-cert.us-cert.gov/advisories/ICSA-17-089-02

15. Siemens RUGGEDCOM VPN Products

https://ics-cert.us-cert.gov/advisories/ICSA-17-087-01

16. Slackware

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.435262
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.438176
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.370121

17. SUSE

https://www.suse.com/support/update/announcement/2017/suse-su-20170839-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170841-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170848-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170853-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170855-1.html

https://www.suse.com/support/update/announcement/2017/suse-su-20170858-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170859-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170860-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170862-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170864-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170865-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170866-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170867-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170868-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170869-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170870-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170871-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170872-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170873-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170874-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170875-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170876-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170877-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170878-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170879-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170880-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170881-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170882-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170883-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170884-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170885-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170886-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170887-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170888-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170889-1.html

18. Ubuntu

https://www.ubuntu.com/usn/usn-3233-1/
https://www.ubuntu.com/usn/usn-3239-3/
https://www.ubuntu.com/usn/usn-3244-1/
https://www.ubuntu.com/usn/usn-3245-1/
https://www.ubuntu.com/usn/usn-3246-1/
https://www.ubuntu.com/usn/usn-3247-1/
https://www.ubuntu.com/usn/usn-3236-1/
https://www.ubuntu.com/usn/usn-3248-1/
https://www.ubuntu.com/usn/usn-3249-1/
https://www.ubuntu.com/usn/usn-3249-2/
https://www.ubuntu.com/usn/usn-3250-1/
https://www.ubuntu.com/usn/usn-3250-2/
https://www.ubuntu.com/usn/usn-3251-1/
https://www.ubuntu.com/usn/usn-3251-2/
https://www.ubuntu.com/usn/usn-3216-2/
https://www.ubuntu.com/usn/usn-3242-2/

19. VMware Products

http://www.vmware.com/security/advisories/VMSA-2017-0006.html

20. **Windows Server 2003 IIS 6.0**
    https://nvd.nist.gov/vuln/detail/CVE-2017-7269
    https://www.us-cert.gov/ncas/current-activity/2017/03/30/Internet-Information-Services-IIS-60-Vulnerability

21. **Xen**
    http://xenbits.xen.org/xsa/advisory-206.html

Sources of product vulnerability information:

Apple
CentOS
Debian
F5
Gentoo
Google Chrome
HKCERT
Huawei
ICS-CERT
IBM
Mageia
NTP
Oracle Linux
Samba
Slackware
SUSE
Ubuntu
US-CERT
VMware
Xen

Contact:

cert@govcert.gov.hk