GovCERT.HK

Weekly IT Security News Bulletin, 2017-W8

20 February – 26 February 2017

Headlines

94% of critical Microsoft vulnerabilities mitigated by removing admin rights

- Endpoint security software vendor, Avecto, released its 2016 Microsoft Vulnerabilities Report, showing that 189 out of a total of 530 vulnerabilities fixed by Microsoft were ranked critical. 94% of these critical vulnerabilities could be mitigated if the admin rights were removed from end user accounts. The same mitigation could work for all Internet Explorer and Edge vulnerabilities and 99% of Microsoft Office vulnerabilities.

- The report also revealed that Windows 10 got 395 vulnerabilities, 46% more than Windows 8 and Windows 8.1, which had 295 each; while Microsoft Office products had 79 vulnerabilities.

- Remote code execution, information disclosure and elevation of privilege were the top three threats of the vulnerabilities.

Advice

- Patch the operating systems and software timely to avoid being exploited via the known vulnerabilities.

- Adopt an approach of least privilege and remove admin rights from end user accounts.

- Avoid using end-of-support operating systems and software since their vulnerabilities would no longer be patched.

Sources

- Avecto
- SecurityWeek

Researchers uncover new leads behind Shamoon2

- In November 2016 and January 2017, the Shamoon 2 attack campaign has made destructive attacks against thousands of computer systems across multiple government and civil organisations in Saudi Arabia and Gulf states. The malware destroyed computer hard drives by wiping the master boot record (MBR) and data irretrievably.

- The attack used the spear phishing technique to deliver a document with malicious macro scripts. The scripts established command and control communications to the attacker's server and enabled remote execution of PowerShell commands. After intruding into the victim organisation's internal network, the attacker deployed additional toolkits and malware to other computers, escalate privileges, study the network and locate critical servers.

- At the final stage, the attacker deployed the Shamoon malware and coordinated the outbreak to wide permanently computer hard drives across the organisation.

Advice

- Disable macros in electronic documents by default and do not enable it unless after confirming that the macros are legitimate from a trusted party.

- Monitor and review the logs of security perimeters for suspicious activities.

- Enforce script execution policy for PowerShell so that all scripts to be run on user computers have to be signed by a Trusted Publisher.

- Maintain offline backup for important data.

Sources

- Threat Post
- IBM Security Intelligence
- GovCERT.HK Security Advisory (S16-01)

Product Vulnerability Notes & Security Updates

1. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-February/022274.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022275.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022276.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022277.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022278.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022279.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022280.html

2. **Debian**
   https://www.debian.org/security/2017/dsa-3790
   http://www.debian.org/security/2017/dsa-3791
   http://www.debian.org/security/2017/dsa-3792

3. **F5 Products**
   https://support.f5.com/csp/article/K54095660
   https://support.f5.com/csp/article/K04450715

4. **FreeBSD**
   https://security.freebsd.org/advisories/FreeBSD-SA-17:02.openssl.asc

5. **Gentoo Linux**
   https://security.gentoo.org/glsa/201702-09
   https://security.gentoo.org/glsa/201702-10
   https://security.gentoo.org/glsa/201702-11
   https://security.gentoo.org/glsa/201702-12
   https://security.gentoo.org/glsa/201702-13
   https://security.gentoo.org/glsa/201702-14
   https://security.gentoo.org/glsa/201702-15
   https://security.gentoo.org/glsa/201702-16
   https://security.gentoo.org/glsa/201702-17
   https://security.gentoo.org/glsa/201702-18
   https://security.gentoo.org/glsa/201702-19
   https://security.gentoo.org/glsa/201702-20
   https://security.gentoo.org/glsa/201702-21
   https://security.gentoo.org/glsa/201702-22
   https://security.gentoo.org/glsa/201702-23
   https://security.gentoo.org/glsa/201702-24
   https://security.gentoo.org/glsa/201702-25
   https://security.gentoo.org/glsa/201702-26
   https://security.gentoo.org/glsa/201702-27
   https://security.gentoo.org/glsa/201702-28
   https://security.gentoo.org/glsa/201702-29
   https://security.gentoo.org/glsa/201702-30
   https://security.gentoo.org/glsa/201702-31
   https://security.gentoo.org/glsa/201702-32

6. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0048.html
   http://advisories.mageia.org/MGASA-2017-0049.html

http://advisories.mageia.org/MGASA-2017-0050.html
http://advisories.mageia.org/MGASA-2017-0051.html
http://advisories.mageia.org/MGASA-2017-0052.html
http://advisories.mageia.org/MGASA-2017-0053.html
http://advisories.mageia.org/MGASA-2017-0054.html
http://advisories.mageia.org/MGASA-2017-0055.html
http://advisories.mageia.org/MGASA-2017-0056.html
http://advisories.mageia.org/MGASA-2017-0057.html
http://advisories.mageia.org/MGASA-2017-0058.html
http://advisories.mageia.org/MGASA-2017-0059.html
http://advisories.mageia.org/MGASA-2017-0060.html
http://advisories.mageia.org/MGASA-2017-0061.html
http://advisories.mageia.org/MGASA-2017-0062.html

7. **Microsoft Products**
   https://technet.microsoft.com/library/security/ms17-feb
   https://technet.microsoft.com/en-us/library/security/MS17-005

8. **openSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00026.html
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00027.html
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00030.html
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00031.html
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00032.html
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00036.html
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00037.html

9. **Oracle Linux**
   https://linux.oracle.com/errata/ELSA-2017-0286.html
   https://linux.oracle.com/errata/ELSA-2017-3518.html
   https://linux.oracle.com/errata/ELSA-2017-3519.html
   https://linux.oracle.com/errata/ELSA-2017-0293.html
   https://linux.oracle.com/errata/ELSA-2017-0294.html

10. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:0286
    https://access.redhat.com/errata/RHSA-2017:0293
    https://access.redhat.com/errata/RHSA-2017:0294
    https://access.redhat.com/errata/RHSA-2017:0295
    https://access.redhat.com/errata/RHSA-2017:0300
    https://access.redhat.com/errata/RHSA-2017:0307
    https://access.redhat.com/errata/RHSA-2017:0309
    https://access.redhat.com/errata/RHSA-2017:0316

11. **Red Lion Controls Sixnet-Managed Industrial Switches, AutomationDirect STRIDE-Managed Ethernet Switches**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-054-02

12. **Schneider Electric Modicon M340 PLC**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-054-03

13. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170490-1.html

https://www.suse.com/support/update/announcement/2017/suse-su-20170494-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170495-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170517-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170518-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170519-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170523-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170529-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170534-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170553-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170554-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170555-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170556-1.html

14. Ubuntu

https://www.ubuntu.com/usn/usn-3199-2/
https://www.ubuntu.com/usn/usn-3202-1/
https://www.ubuntu.com/usn/usn-3203-1/
https://www.ubuntu.com/usn/usn-3204-1/
https://www.ubuntu.com/usn/usn-3205-1/
https://www.ubuntu.com/usn/usn-3206-1/
https://www.ubuntu.com/usn/usn-3207-1/
https://www.ubuntu.com/usn/usn-3207-2/
https://www.ubuntu.com/usn/usn-3208-1/
https://www.ubuntu.com/usn/usn-3208-2/
https://www.ubuntu.com/usn/usn-3209-1/
https://www.ubuntu.com/usn/usn-3142-2/
https://www.ubuntu.com/usn/usn-3210-1/
https://www.ubuntu.com/usn/usn-3211-1/

15. VIPA Controls WinPLC7

https://ics-cert.us-cert.gov/advisories/ICSA-17-054-01

16. Xen

http://xenbits.xen.org/xsa/advisory-209.html
http://xenbits.xen.org/xsa/advisory-210.txt

Sources of product vulnerability information:

- CentOS
- Debian
- F5
- FreeBSD
- Gentoo Linux
- ICS-CERT
- Mageia
- Microsoft
- openSUSE
- Oracle Linux
- Red Hat
- SUSE
- Ubuntu
- Xen

Contacts:

cert@govcert.gov.hk