GovCERT.HK

Weekly IT Security News Bulletin, 2017-W5

30 January – 5 February 2017

Headlines

Cisco 2017 Annual Cybersecurity Report: chief security officers reveal true cost of breaches and the actions organizations are taking

- The report surveyed almost 3,000 chief security officers (CSOs) and the like of 13 countries. The CSOs regarded budget constraints, poor system compatibility and shortage of trained talent as the biggest obstacles to improving security postures.

- The traditional attack vectors such as adware and email spam are back on the rising trend while the hacker operations take up new business models including employing brokers in malvertising campaigns to mask malicious activity and evade detection. More adoption of cloud applications also generates security concerns. There is a drop in the use of large exploit kits such as Angler, Nuclear and Neutrino since their owners were brought down in 2016, but smaller exploit tools are taking the place.

- Cyber attacks could cause organisations to lose customers, revenues and business opportunities. 29% of breached organisations did lose revenue and 38% of them lost over 20% of revenue.

Advice

- In the cyber economy, organisations should take security as a business priority to get well prepared against cyber threats.

- Organisations should establish metrics to review and test the effectiveness of their security operations.

- Defense operations should be integrated and automated as far as possible to increase visibility, streamline interoperability and shorten time to detect and respond to cyber attacks.

Sources

- Cisco's Technology News Site
- Cisco 2017 Annual Cybersecurity Report

Microsoft Windows SMB Tree Connect Response denial of service vulnerability

- On 2 February 2017, the CERT/CC revealed that there was a memory corruption vulnerability in handling of Server Message Block (SMB) network traffic. A remote attacker could exploit this vulnerability by enticing a user to connect to a malicious SMB server which could cause the Windows system to crash, resulting in a denial-of-service condition. Proof-of-concept exploit code for this vulnerability is publicly available.

- The vulnerability was due to improper handling of a specially-crafted server response which contains too many bytes following the structure defined in the SMB2 TREE_CONNECT Response structure.

Advice

- Block outbound SMB connections (TCP ports 139 and 445 along with UDP ports 137 and 138).

- Keep Windows systems updated with the latest patches.

Sources

- CERT/CC
- GitHub (Proof of Concept Exploit Code)

Product Vulnerability Notes & Security Updates

1. **BINOM3 Electric Power Quality Meter**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-031-01

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-February/022259.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022261.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022262.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022263.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022264.html

3. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170130-openssl
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-asrsnmp
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-cbr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-esa1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-fmc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-fpw
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-fpw1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-fpw2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-prime-home
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-psc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170201-psc1

4. **Debian**
   https://www.debian.org/security/2017/dsa-3773
   https://www.debian.org/security/2017/dsa-3774
   https://www.debian.org/security/2017/dsa-3775
   https://www.debian.org/security/2017/dsa-3776
   https://www.debian.org/security/2017/dsa-3777
   https://www.debian.org/security/2017/dsa-3778
   https://www.debian.org/security/2017/dsa-3779
   https://www.debian.org/security/2017/dsa-3780

5. **Ecava IntegraXor**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-031-02

6. **F5 Products**
   https://support.f5.com/csp/article/K05513373
   https://support.f5.com/csp/article/K32743437
   https://support.f5.com/csp/article/K54610514
   https://support.f5.com/csp/article/K62201745
   https://support.f5.com/csp/article/K73705133

7. **Gentoo Linux**
   https://security.gentoo.org/glsa/201701-66
   https://security.gentoo.org/glsa/201701-67
   https://security.gentoo.org/glsa/201701-68
   https://security.gentoo.org/glsa/201701-69

https://security.gentoo.org/glsa/201701-70
https://security.gentoo.org/glsa/201701-71
https://security.gentoo.org/glsa/201701-72
https://security.gentoo.org/glsa/201701-73
https://security.gentoo.org/glsa/201701-74
https://security.gentoo.org/glsa/201701-75
https://security.gentoo.org/glsa/201701-76
https://security.gentoo.org/glsa/201701-77
https://security.gentoo.org/glsa/201702-01

8. **Honeywell XL Web II Controller**
https://ics-cert.us-cert.gov/advisories/ICSA-17-033-01

9. **IBM Products**
http://www-01.ibm.com/support/docview.wss?uid=swg21996759
http://www-01.ibm.com/support/docview.wss?uid=swg21996847

10. **Mageia**
http://advisories.mageia.org/MGASA-2017-0021.html
http://advisories.mageia.org/MGASA-2017-0022.html
http://advisories.mageia.org/MGASA-2017-0023.html
http://advisories.mageia.org/MGASA-2017-0024.html
http://advisories.mageia.org/MGASA-2017-0025.html
http://advisories.mageia.org/MGASA-2017-0026.html
http://advisories.mageia.org/MGASA-2017-0027.html
http://advisories.mageia.org/MGASA-2017-0028.html
http://advisories.mageia.org/MGASA-2017-0029.html
http://advisories.mageia.org/MGASA-2017-0030.html
http://advisories.mageia.org/MGASA-2017-0031.html
http://advisories.mageia.org/MGASA-2017-0032.html
http://advisories.mageia.org/MGASA-2017-0033.html
http://advisories.mageia.org/MGASA-2017-0034.html
http://advisories.mageia.org/MGASA-2017-0035.html
http://advisories.mageia.org/MGASA-2017-0036.html
http://advisories.mageia.org/MGASA-2017-0037.html

11. **Microsoft Windows Server Message Block SMBv3**
https://www.hkcert.org/my_url/en/alert/17020301
http://www.kb.cert.org/vuls/id/867968

12. **Oracle Linux**
https://linux.oracle.com/errata/ELSA-2017-0225.html
https://linux.oracle.com/errata/ELSA-2017-0238.html

13. **openSUSE**
https://lists.opensuse.org/opensuse-security-announce/2017-01/msg00061.html
https://lists.opensuse.org/opensuse-security-announce/2017-01/msg00064.html
https://lists.opensuse.org/opensuse-security-announce/2017-01/msg00066.html
https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00001.html
https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00002.html

14. **Red Hat**
https://access.redhat.com/errata/RHSA-2017:0190
https://access.redhat.com/errata/RHSA-2017:0193

https://access.redhat.com/errata/RHSA-2017:0194
https://access.redhat.com/errata/RHSA-2017:0196
https://access.redhat.com/errata/RHSA-2017:0206
https://access.redhat.com/errata/RHSA-2017:0215
https://access.redhat.com/errata/RHSA-2017:0216
https://access.redhat.com/errata/RHSA-2017:0217
https://access.redhat.com/errata/RHSA-2017:0225
https://access.redhat.com/errata/RHSA-2017:0226
https://access.redhat.com/errata/RHSA-2017:0238
https://access.redhat.com/errata/RHSA-2017:0244
https://access.redhat.com/errata/RHSA-2017:0245
https://access.redhat.com/errata/RHSA-2017:0246
https://access.redhat.com/errata/RHSA-2017:0250

15. SUSE
https://www.suse.com/support/update/announcement/2017/suse-su-20170302-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170303-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170304-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170305-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170307-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170330-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170331-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170333-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170338-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170339-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170340-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170346-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170348-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170366-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170367-1.html

16. Ubuntu
https://www.ubuntu.com/usn/usn-3165-1/
https://www.ubuntu.com/usn/usn-3175-1/
https://www.ubuntu.com/usn/usn-3181-1/
https://www.ubuntu.com/usn/usn-3182-1/
https://www.ubuntu.com/usn/usn-3183-1/
https://www.ubuntu.com/usn/usn-3184-1/
https://www.ubuntu.com/usn/usn-3185-1/
https://www.ubuntu.com/usn/usn-3186-1/
https://www.ubuntu.com/usn/usn-3177-2/

17. WMware Airwatch Agent for Android
http://www.vmware.com/security/advisories/VMSA-2017-0001.html

Sources of product vulnerability information:

- CERT/CC
- Cisco
- CentOS
- Debian
- F5
- Gentoo
- HKCERT
- IBM
- ICS-CERT
- Mageia
- openSUSE
- Oracle Linux
- Red Hat
- SUSE
- Ubuntu
- VMware

Contacts:

cert@govcert.gov.hk