GovCERT.HK

Weekly IT Security News Bulletin, 2017-W33

14 August – 20 August 2017

Headlines

New PowerPoint attack with old flaw

- In April 2017, Microsoft disclosed a remote code execution vulnerability (CVE-2017-0199) in its Office and WordPad software, which could be exploited when a user opens or previews a specially crafted file in Rich Text File (RTF) format with the software. An attacker could then install programs; read, modify or remove data; or create accounts with full user rights on the affected system. The DRIDEX banking trojan was previously found using the method to infect computers.

- In addition to the RTF attack method, the PowerPoint Open XML Slide Show (PPTX) file was recently discovered as a new attack vector to exploit the same vulnerability. A malicious PPTX attachment was delivered by a phishing email, which bluffed the recipient into opening the PPTX file. PowerPoint then ran the remote malicious payload via the PowerPoint Show animations feature to exploit the vulnerability and download further hacker tools such as key loggers, screen loggers and recorders for webcam and microphone, for remote execution.

- With the new attack vector, the attacker may evade anti-malware detections focusing on the RTF method. Whatsoever, the patch to fix the vulnerability has been available from Microsoft in April 2017. Computers installed with the latest patches are safe from both attack methods.

Advice

- Ensure your Microsoft Office products have been installed with the latest patches, including that for CVE-2017-0199.

- Keep your anti-malware engines and signatures update.

- Do not open any attachments or click on any links from unsolicited emails.

Sources

- Trend Micro
- Microsoft

Millions open ports for publicly accessible remote desktops

- A recent study conducted by a cybersecurity vendor revealed that 4.1 million computer systems allowed access over the Internet using the remote desktop protocol (RDP), which is pre-installed in all current Microsoft Windows versions.

- RDP enables user access to the virtual screen, keyboard and mouse of a remote computer with TCP port 3389 open. The powerful remote control capabilities make RDP a favourite administrator tool as well as a prime target for hackers. There are reports indicating that RDP is an increasingly popular distribution vector for ransomware.

- The study also revealed that over 83% of the RDP-enabled systems identified could support the more secure Credential Security Support Provider (CredSSP) and Transport Layer Security (TLS) protocols to authenticate and protect the RDP session, while more than 15% did not run Secure Socket Layer (SSL) or TLS, leaving them susceptible to man-in-the-middle attacks.

Advice

- Disable RDP service on computer systems, if not necessary.

- Block TCP port 3389 at Internet firewalls or routers by default to avoid universal access and allow access only from specific source IPs on need basis.

- Update Windows operating systems to supported versions with latest patches to ensure stronger security protocols are supported and known loopholes fixed.

- If there is a genuine need to use RDP service over the Internet, use more secure protocols such as CredSSP and TLS, together with virtual private network solutions to better authenticate and protect RDP sessions.

Sources

- Rapid7
- Bleeping Computer
- SecurityWeek

Product Vulnerability Notes & Security Updates

1. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-August/022516.html
   https://lists.centos.org/pipermail/centos-announce/2017-August/022517.html
   https://lists.centos.org/pipermail/centos-announce/2017-August/022518.html
   https://lists.centos.org/pipermail/centos-announce/2017-August/022519.html

2. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-caw
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-cpi
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-cps
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-crr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-csa
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-em
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-esc1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-esc2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-esc3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-esc4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-staros1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-staros2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-staros3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-ucm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-usf
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-usp
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-vcs

3. **Debian**
   https://www.debian.org/security/2017/dsa-3935
   https://www.debian.org/security/2017/dsa-3936
   https://www.debian.org/security/2017/dsa-3937
   https://www.debian.org/security/2017/dsa-3938
   https://www.debian.org/security/2017/dsa-3939
   https://www.debian.org/security/2017/dsa-3940
   https://www.debian.org/security/2017/dsa-3941
   https://www.debian.org/security/2017/dsa-3942
   https://www.debian.org/security/2017/dsa-3943
   https://www.debian.org/security/2017/dsa-3944
   https://www.debian.org/security/2017/dsa-3945

4. **Drupal**
   https://www.drupal.org/SA-CORE-2017-004

5. **Gentoo Linux**
   https://security.gentoo.org/glsa/201708-01
   https://security.gentoo.org/glsa/201708-02

6. **IBM WebSphere Application Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg22006810

7. **Mageia**

http://advisories.mageia.org/MGASA-2017-0255.html
http://advisories.mageia.org/MGASA-2017-0256.html
http://advisories.mageia.org/MGASA-2017-0257.html
http://advisories.mageia.org/MGASA-2017-0258.html
http://advisories.mageia.org/MGASA-2017-0259.html
http://advisories.mageia.org/MGASA-2017-0260.html
http://advisories.mageia.org/MGASA-2017-0261.html
http://advisories.mageia.org/MGASA-2017-0262.html
http://advisories.mageia.org/MGASA-2017-0263.html
http://advisories.mageia.org/MGASA-2017-0264.html
http://advisories.mageia.org/MGASA-2017-0265.html
http://advisories.mageia.org/MGASA-2017-0266.html
http://advisories.mageia.org/MGASA-2017-0267.html
http://advisories.mageia.org/MGASA-2017-0268.html
http://advisories.mageia.org/MGASA-2017-0269.html
http://advisories.mageia.org/MGASA-2017-0270.html
http://advisories.mageia.org/MGASA-2017-0271.html
http://advisories.mageia.org/MGASA-2017-0272.html
http://advisories.mageia.org/MGASA-2017-0273.html
http://advisories.mageia.org/MGASA-2017-0274.html
http://advisories.mageia.org/MGASA-2017-0275.html
http://advisories.mageia.org/MGASA-2017-0276.html

8. **openSUSE**

https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00042.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00043.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00044.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00046.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00047.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00050.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00051.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00052.html

9. **Oracle Linux**

https://linux.oracle.com/errata/ELSA-2017-1842-1.html
https://linux.oracle.com/errata/ELSA-2017-2456.html
https://linux.oracle.com/errata/ELSA-2017-2471.html
https://linux.oracle.com/errata/ELSA-2017-2473-1.html
https://linux.oracle.com/errata/ELSA-2017-2473.html
https://linux.oracle.com/errata/ELSA-2017-2478.html
https://linux.oracle.com/errata/ELSA-2017-2479.html
https://linux.oracle.com/errata/ELSA-2017-2480.html
https://linux.oracle.com/errata/ELSA-2017-2484.html
https://linux.oracle.com/errata/ELSA-2017-2485.html
https://linux.oracle.com/errata/ELSA-2017-2486.html
https://linux.oracle.com/errata/ELSA-2017-2489.html
https://linux.oracle.com/errata/ELSA-2017-3605.html

10. **Philips' DoseWise Portal**

https://ics-cert.us-cert.gov/advisories/ICSMA-17-229-01

11. **Red Hat**

https://access.redhat.com/errata/RHSA-2017:2469
https://access.redhat.com/errata/RHSA-2017:2471
https://access.redhat.com/errata/RHSA-2017:2472
https://access.redhat.com/errata/RHSA-2017:2473
https://access.redhat.com/errata/RHSA-2017:2477
https://access.redhat.com/errata/RHSA-2017:2478
https://access.redhat.com/errata/RHSA-2017:2479
https://access.redhat.com/errata/RHSA-2017:2480
https://access.redhat.com/errata/RHSA-2017:2481
https://access.redhat.com/errata/RHSA-2017:2483
https://access.redhat.com/errata/RHSA-2017:2484
https://access.redhat.com/errata/RHSA-2017:2485
https://access.redhat.com/errata/RHSA-2017:2486
https://access.redhat.com/errata/RHSA-2017:2489
https://access.redhat.com/errata/RHSA-2017:2491

12. **Slackware**

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.1288055
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.383531
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.432714
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.449586
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.575003

13. **SUSE**

https://www.suse.com/support/update/announcement/2017/suse-su-20172131-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172141-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172142-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172143-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172144-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172150-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172163-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172168-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172173-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172174-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172175-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172176-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172199-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172200-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172201-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172202-1.html

14. **Symantec Messaging Gateway**

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20170810_00
https://www.us-cert.gov/ncas/current-activity/2017/08/11/Symantec-Releases-Security-Update

15. **Ubuntu**

https://usn.ubuntu.com/usn/usn-3387-1/
https://usn.ubuntu.com/usn/usn-3388-1/
https://usn.ubuntu.com/usn/usn-3389-1/
https://usn.ubuntu.com/usn/usn-3389-2/
https://usn.ubuntu.com/usn/usn-3390-1/
https://usn.ubuntu.com/usn/usn-3391-1/
https://usn.ubuntu.com/usn/usn-3391-2/
https://usn.ubuntu.com/usn/usn-3392-1/
https://usn.ubuntu.com/usn/usn-3392-2/
https://usn.ubuntu.com/usn/usn-3391-3/
https://usn.ubuntu.com/usn/usn-3393-1/
https://usn.ubuntu.com/usn/usn-3393-2/
https://usn.ubuntu.com/usn/usn-3394-1/
https://usn.ubuntu.com/usn/usn-3395-1/

16. **Xen**

http://xenbits.xen.org/xsa/advisory-226.html
http://xenbits.xen.org/xsa/advisory-227.html
http://xenbits.xen.org/xsa/advisory-228.html
http://xenbits.xen.org/xsa/advisory-229.html
http://xenbits.xen.org/xsa/advisory-230.html

Sources of product vulnerability information:

CentOS
Cisco Products
Debian
Drupal
Gentoo Linux
IBM
ICS-CERT
Mageia
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Symantec
Ubuntu
US-CERT
Xen

Contacts:

cert@govcert.gov.hk