GovCERT.HK

Weekly IT Security News Bulletin, 2017-W43

23 October – 29 October 2017

Headlines

Bad Rabbit ransomware hopping across Europe

- A new ransomware known as "Bad Rabbit" struck multiple organisations across Eastern Europe and Russia on 24 October 2017. It was spread through compromised websites, where visiting users were redirected to download a fake Adobe Flash Player update. After the update was executed by an unsuspecting user, the malware dropped additional malicious payloads for running on the infected computer.

- Bad Rabbit moved across the local area network via legitimate features of Microsoft Windows, including Windows Management Instrumentation (WMI) and Server Message Block (SMB). The EternalRomance exploit was also used to enable the spreading. The exploit could bypass security over SMB file-sharing connections to execute instructions remotely on Windows systems. Furthermore, the malware carried a list of weak credentials and the mimikatz password dumping tool to force its way into computers across the network.

- Meanwhile, another attack campaign was exploiting the latest disclosed Adobe Flash vulnerability, CVE-2017-11292 to cause arbitrary code execution across Windows, Mac OS, Linux, and Chrome OS systems. While it is essential to patch the Adobe Flash without delay, the patch must be acquired from trustworthy sources to avoid falling prey to the Bad Rabbit attack or the like, which distributed fake Flash updates.

Advice

- Apply latest security patches on Windows systems to defend against known exploits, such as EthernalRomance; and update Adobe Flash Player to the latest version to fix the CVE-2017-11292 vulnerability, using patches/updates from their respective official websites.

- Block the SMB ports (TCP ports 139 and 445) from Internet access.

- Back up data regularly and keep the backup storage offline.

Sources

- Cisco Talos
- Proofpoint
- Microsoft Security Bulletin
- Adobe Security Bulletin

DDE as attack vector in malware campaigns

- The Dynamic Data Exchange (DDE) protocol allows a Microsoft Office application to load data from the other Office applications. It works through a DDE field inserted into a document, containing instructions on where to pull data and what data to inject into the document. For instance, a Word document can use DDE to update a table by pulling data from an Excel spreadsheet every time the Word document is opened.

- Recent attack campaigns were discovered deploying DDE to spread malware in Microsoft Word documents, as an alternative technique to running malicious macros. Attackers create Office documents with DDE fields that open a command prompt and run malicious code, instead of opening another Office application. The DDE attack has been adopted in malware campaigns involving DNSMessenger Trojan, Hancitor malware and Locky ransomware.

- Microsoft Office applications will prompt two warnings to users under the DDE attack. The first alerts that the document contains links to the other files while the second asks whether the users would like to open a command prompt for code execution. Only if users are used to dismiss the warnings that pop up can malicious commands embedded in the DDE fields get executed.

Advice

- Avoid opening Office documents from unknown sources, such as attachments of unsolicited emails.

- Think twice before dismissing warnings prompted by the system when opening documents.

- Open received documents by a user account without administrative privileges to contain the impact of the DDE attack or the like.

Sources

- SensePost
- The Hacker News: 12 October, 19 October
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-October/022571.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022601.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022603.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022605.html

2. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171020-ampfe
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171023-spark

3. **Debian**
   https://www.debian.org/security/2017/dsa-4004
   https://www.debian.org/security/2017/dsa-4005
   https://www.debian.org/security/2017/dsa-4006

4. **F5 Products**
   https://support.f5.com/csp/article/K02692210
   https://support.f5.com/csp/article/K10002335
   https://support.f5.com/csp/article/K13421245
   https://support.f5.com/csp/article/K19430431
   https://support.f5.com/csp/article/K22541983
   https://support.f5.com/csp/article/K30201296
   https://support.f5.com/csp/article/K39909763
   https://support.f5.com/csp/article/K62279530

5. **Fortinet FortiOS**
   https://fortiguard.com/psirt/FG-IR-17-113
   https://fortiguard.com/psirt/FG-IR-17-206

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201710-21
   https://security.gentoo.org/glsa/201710-22
   https://security.gentoo.org/glsa/201710-23
   https://security.gentoo.org/glsa/201710-24
   https://security.gentoo.org/glsa/201710-25
   https://security.gentoo.org/glsa/201710-26
   https://security.gentoo.org/glsa/201710-27

7. **Google Chrome**
   https://chromereleases.googleblog.com/2017/10/stable-channel-update-for-desktop_26.html

8. **Huawei Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171025-01-firewall-en
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171025-01-gaussdb-en

9. **IBM WebSphere Application Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg22008707

10. **Korenix JetNet**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-299-01

11. **Mageia**

http://advisories.mageia.org/MGASA-2017-0382.html
http://advisories.mageia.org/MGASA-2017-0383.html
http://advisories.mageia.org/MGASA-2017-0384.html
http://advisories.mageia.org/MGASA-2017-0385.html
http://advisories.mageia.org/MGASA-2017-0386.html
http://advisories.mageia.org/MGASA-2017-0387.html
http://advisories.mageia.org/MGASA-2017-0388.html

12. **openSUSE**

https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00069.html
https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00072.html

13. **Oracle Linux**

https://linux.oracle.com/errata/ELSA-2017-2998.html
https://linux.oracle.com/errata/ELSA-2017-2930-1.html
https://linux.oracle.com/errata/ELSA-2017-3071.html
https://linux.oracle.com/errata/ELSA-2017-3075.html
https://linux.oracle.com/errata/ELSA-2017-3631.html
https://linux.oracle.com/errata/ELSA-2017-3632.html
https://linux.oracle.com/errata/ELSA-2017-3633.html

14. **Red Hat**

https://access.redhat.com/errata/RHSA-2017:2997
https://access.redhat.com/errata/RHSA-2017:2998
https://access.redhat.com/errata/RHSA-2017:2999
https://access.redhat.com/errata/RHSA-2017:3002
https://access.redhat.com/errata/RHSA-2017:3005
https://access.redhat.com/errata/RHSA-2017:3018
https://access.redhat.com/errata/RHSA-2017:3046
https://access.redhat.com/errata/RHSA-2017:3047
https://access.redhat.com/errata/RHSA-2017:3071
https://access.redhat.com/errata/RHSA-2017:3075

15. **Slackware**

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.421440
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.439610

16. **SUSE**

https://www.suse.com/security/cve/CVE-2017-12762/
https://www.suse.com/support/update/announcement/2017/suse-su-20172812-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172813-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172815-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172831-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172838-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172839-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172847-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172850-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172854-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172855-1/

https://www.suse.com/support/update/announcement/2017/suse-su-20172856-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172860-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172861-1/

17. Ubuntu

https://usn.ubuntu.com/usn/usn-3388-2/
https://usn.ubuntu.com/usn/usn-3411-2/
https://usn.ubuntu.com/usn/usn-3425-2/
https://usn.ubuntu.com/usn/usn-3434-2/
https://usn.ubuntu.com/usn/usn-3441-2/
https://usn.ubuntu.com/usn/usn-3454-2/
https://usn.ubuntu.com/usn/usn-3457-1/
https://usn.ubuntu.com/usn/usn-3458-1/
https://usn.ubuntu.com/usn/usn-3458-2/
https://usn.ubuntu.com/usn/usn-3459-1/
https://usn.ubuntu.com/usn/usn-3460-1/
https://usn.ubuntu.com/usn/usn-3461-1/
https://usn.ubuntu.com/usn/usn-3462-1/
https://usn.ubuntu.com/usn/usn-3463-1/
https://usn.ubuntu.com/usn/usn-3464-1/
https://usn.ubuntu.com/usn/usn-3465-1/
https://usn.ubuntu.com/usn/usn-3466-1/

18. Xen

http://xenbits.xen.org/xsa/advisory-236.html

Sources of product vulnerability information:

CentOS
Cisco
Debian
F5
Fortinet
Gentoo Linux
Google Chrome
Huawei
IBM
ICS-CERT
Mageia
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
Xen

Contacts:

cert@govcert.gov.hk