GovCERT.HK

Weekly IT Security News Bulletin, 2017-W21

22 May – 28 May 2017

Headlines

EternalRocks spreads through additional Shadow Brokers exploits

- EternalRocks (also called BlueDoom) is a network worm that spreads through four Server Message Block (SMB) exploits (EternalBlue, EternalChampion, EternalRomance and EternalSynergy), along with three related programs (DoublePulsar, Architouch and SMBTouch), publicly released by the hacker group Shadow Brokers. The vulnerabilities exploited have been fixed by the Microsoft Windows MS17-010 patches. In contrast, the WannaCry malware uses EternalBlue and DoublePulsar only. Furthermore, WannaCry is a crypto ransomware while EternalRocks is a Trojan without any other malicious payload observed so far.

- EternalRocks infects computers by two stages. In the first stage, it gets through the remote SMB exploitation, downloads and installs necessary software to run Tor[1] process for establishing a communication channel with the command-and-control (C&C) server on the Dark Web. In the second stage, it goes dormant for 24 hours to evade sandbox detection and then downloads the SMB exploits from the C&C server to scan for open TCP port 445 on the next victims in the Internet.

- On 25 May 2017, it was found that EternalRocks has changed its mode of operation. It only downloads a dummy program that executes nothing instead of the SMB exploits from its C&C server. Newly infected computers are therefore not able to spread to others. Previously infected computers will continue to scan for new victims, which, without the exploits, will however stop further spreading.

Advice

- Apply latest security patches, especially MS17-010, on all Windows-based systems, including Windows XP, Windows Server 2003 and above.

- Block the access to TCP port 445 from the Internet.

- Keep the anti-malware software and signatures up-to-date on all computers.

Sources

- GitHub - Stamparm/EternalRocks
- Bleeping Computer
- Microsoft TechNet
- Heimdal Security

[1] Tor stands for "**T**he **O**nion **R**outer" and is a worldwide network of servers that enables anonymous Internet browsing. It is also abused by cyber criminals to cover their tracks against law enforcement investigation.

SambaCry? No panic and fix it

- Samba is an open source software implementation of the Server Message Block (SMB) protocols on platforms other than Microsoft Windows, such as Linux and UNIX, to provide file and print sharing services to Microsoft Windows clients. Major Linux/UNIX operating systems (OS) have Samba as a native package for optional installation. Samba is also commonly used in network-attached storage (NAS) devices for file sharing and data backup.

- Samba has a 7-year-old vulnerability (CVE-2017-7494), which allows authenticated malicious clients to upload a shared library and execute it remotely on a Samba server. All Samba versions from 3.5.0 onwards are affected. A patch has been posted on the Samba website on 24.5.2017. A workaround configuration is also provided to disable client access of named pipe endpoints to prevent the remote code execution. Another workaround for some Linux distribution is to mount the file system hosting the Samba writable shares with a "noexec" option.

- In a recent vulnerability scan run by Rapid7 Labs, around 104,000 and 110,000 Internet-facing devices were found running vulnerable Samba versions on TCP port 445 and 139 respectively. The proof-of-concept exploit code has also been available on the Internet.

Advice

- Refer to the Linux /UNIX OS or NAS vendors for applying appropriate patches and upgrade de-supported systems to supported versions before patching, if necessary.

- Implement the workaround measures if patching cannot be done immediately.

- Block the access to TCP ports 445 and 139 from the Internet.

- Perform regular data backup and keep the backup copies disconnected from the network and computer.

Sources

- Samba
- GitHub – Proof-of-concept exploit
- Red Hat Bugzilla
- Rapid7

Persirai 惡意程式肆虐　IP Cam 或會成為殭屍網絡一員

- 根據網絡保安公司趨勢科技近月發表的報告，發現一種名為 Persirai 的物聯網殭屍網絡攻擊，有機會威脅超過 120,000 部網絡攝影機（IP Cam）。報告同時指出，本港約有 5,600 部存有漏洞的網絡攝影機連接着互聯網，這些裝置或會因此遭受 Persirai 入侵。

- 現時大多數網絡攝影機都有提供隨插即用（UPnP）的功能，當網絡攝影機連接到一般家用網絡而沒有採取相應的保護措施，裝置或會於用戶不知情下直接曝露於互聯網上。Persirai 於互聯網隨機搜尋有開啟管理界面連接埠 80 的裝置並發出攻擊指令，由此入侵有安全漏洞或沒有更改預設安全密碼的網絡攝影機。

- 被入侵的裝置會成為其殭屍網絡一員，並用作入侵更多的網絡攝影機。黑客可以發出遙距指令使殭屍網絡內的成員發動分布式拒絕服務攻擊（DDoS attack）以癱瘓目標，例如網站、域名伺服器等。

Advice

- 保持為網絡裝置安裝最新的保安修補程式或固件(firmware)。

- 於初次使用網絡裝置之前，應即時更改預設用戶名稱和密碼。密碼應使用較複雜的組合，例如由至少 8 個大小寫不一的字母、數字及特殊字符混合組成。

- 使用防火牆或路由器的接達控制功能保護網絡內的裝置，防止裝置及其管理界面直接曝露於互聯網上，以阻隔網絡攻擊。

Sources

- 趨勢科技
- 東方日報

Product Vulnerability Notes & Security Updates

1. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-May/022412.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022413.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022414.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022415.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022416.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022417.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022418.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022419.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022420.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022441.html

2. **Cisco Firepower System Software**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170524-fmc

3. **Debian**
   https://www.debian.org/security/2017/dsa-3856
   https://www.debian.org/security/2017/dsa-3857
   https://www.debian.org/security/2017/dsa-3858
   https://www.debian.org/security/2017/dsa-3859
   https://www.debian.org/security/2017/dsa-3860
   https://www.debian.org/security/2017/dsa-3861

4. **IBM**
   http://www-01.ibm.com/support/docview.wss?uid=swg22000516
   http://www-01.ibm.com/support/docview.wss?uid=swg22000602

5. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0140.html
   http://advisories.mageia.org/MGASA-2017-0141.html
   http://advisories.mageia.org/MGASA-2017-0142.html
   http://advisories.mageia.org/MGASA-2017-0143.html
   http://advisories.mageia.org/MGASA-2017-0144.html
   http://advisories.mageia.org/MGASA-2017-0145.html

6. **Moxa OnCell**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-143-01

7. **openSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00059.html
   https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00067.html
   https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00069.html

8. **Oracle Linux**
   https://linux.oracle.com/errata/ELSA-2017-1262.html
   https://linux.oracle.com/errata/ELSA-2017-1263.html
   https://linux.oracle.com/errata/ELSA-2017-1264.html
   https://linux.oracle.com/errata/ELSA-2017-1265.html
   https://linux.oracle.com/errata/ELSA-2017-1267.html
   https://linux.oracle.com/errata/ELSA-2017-1268.html

https://linux.oracle.com/errata/ELSA-2017-1270.html
https://linux.oracle.com/errata/ELSA-2017-1271.html
https://linux.oracle.com/errata/ELSA-2017-3574.html
https://linux.oracle.com/errata/ELSA-2017-3575.html
https://linux.oracle.com/errata/ELSA-2017-3576.html

9. **Red Hat**

https://access.redhat.com/errata/RHSA-2017:1262
https://access.redhat.com/errata/RHSA-2017:1263
https://access.redhat.com/errata/RHSA-2017:1264
https://access.redhat.com/errata/RHSA-2017:1265
https://access.redhat.com/errata/RHSA-2017:1267
https://access.redhat.com/errata/RHSA-2017:1268
https://access.redhat.com/errata/RHSA-2017:1270
https://access.redhat.com/errata/RHSA-2017:1271
https://access.redhat.com/errata/RHSA-2017:1272
https://access.redhat.com/errata/RHSA-2017:1273
https://access.redhat.com/errata/RHSA-2017:1285
https://access.redhat.com/errata/RHSA-2017:1297
https://access.redhat.com/errata/RHSA-2017:1298
https://access.redhat.com/errata/RHSA-2017:1308
https://access.redhat.com/errata/RHSA-2017:1334

10. **Rockwell Automation Allen-Bradley MicroLogix 1100 and 1400**

https://ics-cert.us-cert.gov/advisories/ICSA-17-115-04

11. **Samba**

https://www.samba.org/samba/security/CVE-2017-7494.html
https://www.hkcert.org/my_url/en/alert/17052501

12. **Slackware**

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.513769

13. **SUSE**

https://www.suse.com/support/update/announcement/2017/suse-su-20171346-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171347-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171349-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171351-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171352-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171357-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171360-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171365-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171366-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171367-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171368-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171379-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171382-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171384-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171385-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171386-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171387-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171389-1.html

https://www.suse.com/support/update/announcement/2017/suse-su-20171391-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171392-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171393-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171396-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171398-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171400-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171404-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171411-1.html

14. **Trend Micro ServerProtect for Linux 3.0**
    https://success.trendmicro.com/solution/1117411

15. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3283-2/
    https://www.ubuntu.com/usn/usn-3296-1/
    https://www.ubuntu.com/usn/usn-3296-2/
    https://www.ubuntu.com/usn/usn-3297-1/
    https://www.ubuntu.com/usn/usn-3298-1/
    https://www.ubuntu.com/usn/usn-3298-2/
    https://www.ubuntu.com/usn/usn-3299-1/

16. **VMware Products**
    http://www.vmware.com/security/advisories/VMSA-2017-0009.html

Sources of product vulnerability information:

CentOS
Cisco
Debian
HKCERT
IBM
ICS-CERT
Mageia
openSUSE
Oracle Linux
Red Hat
Samba
Slackware
SUSE
Trend Micro
Ubuntu
VMWare

Contacts:

cert@govcert.gov.hk