GovCERT.HK

Weekly IT Security News Bulletin, 2017-W46

13 November – 19 November 2017

Headlines

#AVGater: Anti-malware flaw causing local privilege escalation

- An Austria-based information security auditor found a new type of vulnerability in multiple Anti-Virus (AV) solutions, which can be exploited by a non-privileged user to gain local admin privileges on a Windows computer. The vulnerability, named "#AVGater", was presented at the IT-Security Community Xchange 2017 (IT-SECX 2017) conference on 10 November 2017.

- The exploitation starts with a malicious dynamic-link (DLL) library file deliberately saved on the target computer by the attacker. The AV software detects the file and moves it to the AV quarantine. The attacker then uses Windows' mklink command to create a NTFS directory junction to redirect the original source path to a system folder, such as C:\Program Files or C:\Windows. The AV software is then called to restore the quarantined file. The restore operation, running with system privilege, saves the file into the write-protected system folder. Privileged Windows processes will subsequently load the malicious DDL library from the system folder to execute the attacker's code with escalated privileges.

- Six AV solutions, including Emisoft, Ikarus, Kaspersky, Malwarebytes, Trend Micro, and ZoneAlarm, were reported to be vulnerable and all of them have released their fixes. Microsoft announced that their Windows Defender Antivirus and other anti-malware products are not impacted. According to the auditor, other AV solutions from different vendors are also affected but their names would be disclosed only after they have fixed the issue.

Advice

- Install AV software updates timely to patch the vulnerability.

- Do not allow non-privileged users to restore previously quarantined files.

Sources

- Bogner Blog
- Ars Technica
- Microsoft
- Twitter

One third of attacks on endpoints would be fileless in 2018

- The 2017 State of Endpoint Security Risk Report from the Ponemon Institute indicates that 29% of endpoint attacks in 2017 were fileless, up from 20% in 2016, and the figure would rise to 35% in 2018. The report, commissioned by endpoint protection firm Barkly, provides findings from a survey of 665 IT security professionals in defence of their organisations against security risks.

- Instead of downloading and installing malicious executable files detectable by anti-malware scanners, the fileless attack runs exploits or launch scripts directly from memory to infect the endpoint without leaving artifacts that could be easily discovered. Legitimate system tools and processes at the infected endpoint may then be abused to gain persistent footholds, escalate access privileges and enable lateral movement across the network.

- The report states that fileless attacks were almost ten times more successful that file-based attacks in compromising the survey respondents' data and IT infrastructure. 77% of the compromises involved fileless techniques. The traditional endpoint security solutions rely on file scanning and signature matching and are therefore ineffective at stopping the evolving attacks. Solutions designed to block new threats like fileless attacks are required to fill the gap in protection.

Advice

- Adopt multiple layers of security protection at endpoints, servers, networks and Internet gateways to address various and evolving attacks.

- Test and deploy new endpoint security solutions that do not only rely on file scanning and signature matching; such as those using machine learning and behavioural analytics to detect and block malicious activities.

- Keep operating systems and other software up-to-date with the latest patches to avoid being exploited at known vulnerabilities.

Sources

- Ponemon Report
- Barkly
- SecurityWeek

Product Vulnerability Notes & Security Updates

1. **Adobe Flash Player and Adobe Reader/Acrobat**
   https://helpx.adobe.com/security/products/acrobat/apsb17-36.html
   https://helpx.adobe.com/security/products/flash-player/apsb17-33.html
   https://www.hkcert.org/my_url/en/alert/17111502

2. **Apple iOS**
   https://support.apple.com/kb/HT208282

3. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-November/022613.html
   https://lists.centos.org/pipermail/centos-announce/2017-November/022624.html

4. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-cms
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-cpt
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-esa
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-findit
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-firepower1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-firepower2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-hyperflex
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-iami
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-ios
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-ipp
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-ise
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-res
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-rf-gateway-1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-spark
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-ucm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-uva
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-vos
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-wsa

5. **Debian**
   https://www.debian.org/security/2017/dsa-4031
   https://www.debian.org/security/2017/dsa-4032
   https://www.debian.org/security/2017/dsa-4033
   https://www.debian.org/security/2017/dsa-4034
   https://www.debian.org/security/2017/dsa-4035
   https://www.debian.org/security/2017/dsa-4036
   https://www.debian.org/security/2017/dsa-4037
   https://www.debian.org/security/2017/dsa-4038
   https://www.debian.org/security/2017/dsa-4039

6. **F5 Products**
   https://support.f5.com/csp/article/K04734043
   https://support.f5.com/csp/article/K05911127

https://support.f5.com/csp/article/K23489380
https://support.f5.com/csp/article/K54747614
https://support.f5.com/csp/article/K56450659
https://support.f5.com/csp/article/K95208524

7. **FreeBSD**
   https://www.freebsd.org/security/advisories/FreeBSD-SA-17:08.ptrace.asc
   https://www.freebsd.org/security/advisories/FreeBSD-SA-17:09.shm.asc
   https://www.freebsd.org/security/advisories/FreeBSD-SA-17:10.kldstat.asc

8. **Gentoo Linux**
   https://security.gentoo.org/glsa/201711-02
   https://security.gentoo.org/glsa/201711-03
   https://security.gentoo.org/glsa/201711-04
   https://security.gentoo.org/glsa/201711-05
   https://security.gentoo.org/glsa/201711-06
   https://security.gentoo.org/glsa/201711-07
   https://security.gentoo.org/glsa/201711-08
   https://security.gentoo.org/glsa/201711-09
   https://security.gentoo.org/glsa/201711-10
   https://security.gentoo.org/glsa/201711-11
   https://security.gentoo.org/glsa/201711-12

9. **IBM WebSphere Application Server Liberty**
   http://www-01.ibm.com/support/docview.wss?uid=swg22010415

10. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0406.html
    http://advisories.mageia.org/MGASA-2017-0407.html
    http://advisories.mageia.org/MGASA-2017-0408.html
    http://advisories.mageia.org/MGASA-2017-0409.html
    http://advisories.mageia.org/MGASA-2017-0410.html
    http://advisories.mageia.org/MGASA-2017-0411.html
    http://advisories.mageia.org/MGASA-2017-0412.html

11. **Microsoft Products**
    https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/bae9d0d8-e497-e711-80e5-000d3a32fc99
    https://support.microsoft.com/en-us/help/20171114/security-update-deployment-information-november-14-2017
    https://www.hkcert.org/my_url/en/alert/17111501

12. **Moxa NPort**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-320-01

13. **Mozilla Firefox**
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-24/
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-25/

14. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00019.html
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00020.html
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00022.html

https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00025.html
https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00028.html

15. **Oracle Linux**
https://linux.oracle.com/errata/ELSA-2017-3200.html
https://linux.oracle.com/errata/ELSA-2017-3221.html
https://linux.oracle.com/errata/ELSA-2017-3640.html

16. **Philips IntelliSpace Cardiovascular System and Xcelera System**
https://ics-cert.us-cert.gov/advisories/ICSMA-17-318-01

17. **Red Hat**
https://access.redhat.com/errata/RHSA-2017:3189
https://access.redhat.com/errata/RHSA-2017:3190
https://access.redhat.com/errata/RHSA-2017:3193
https://access.redhat.com/errata/RHSA-2017:3194
https://access.redhat.com/errata/RHSA-2017:3195
https://access.redhat.com/errata/RHSA-2017:3200
https://access.redhat.com/errata/RHSA-2017:3221
https://access.redhat.com/errata/RHSA-2017:3222

18. **Siemens SICAM**
https://ics-cert.us-cert.gov/advisories/ICSA-17-320-02

19. **SUSE**
https://www.suse.com/support/update/announcement/2017/suse-su-20172327-2/
https://www.suse.com/support/update/announcement/2017/suse-su-20172871-2/
https://www.suse.com/support/update/announcement/2017/suse-su-20172872-2/
https://www.suse.com/support/update/announcement/2017/suse-su-20172963-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172964-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172968-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172969-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172971-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172981-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172989-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172996-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20173000-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20173025-1/

20. **Ubuntu**
https://usn.ubuntu.com/usn/usn-3276-3/
https://usn.ubuntu.com/usn/usn-3477-1/
https://usn.ubuntu.com/usn/usn-3478-1/
https://usn.ubuntu.com/usn/usn-3478-2/
https://usn.ubuntu.com/usn/usn-3479-1/
https://usn.ubuntu.com/usn/usn-3480-1/
https://usn.ubuntu.com/usn/usn-3481-1/
https://usn.ubuntu.com/usn/usn-3482-1/

21. **VMware vCenter Server**
https://www.vmware.com/security/advisories/VMSA-2017-0017.html

Sources of product vulnerability information:

- Adobe
- Apple
- CentOS
- Cisco
- Debian
- F5
- FreeBSD
- Gentoo Linux
- HKCERT
- IBM
- ICS-CERT
- Mageia
- Microsoft
- Mozilla Firefox
- openSUSE
- Oracle Linux
- Red Hat
- SUSE
- Ubuntu
- VMware

Contacts:

cert@govcert.gov.hk