GovCERT.HK

Weekly IT Security News Bulletin, 2017-W6

6 February – 12 February 2017

Headlines

How e-mail filtering helps defend against malware and ransomware

- Nowadays, cyber attackers embed malware and ransomware into e-mails to launch malware attacks which aim at stealing personal information and encrypting your data files. E-mail filters could be used to improve the ability in safeguarding against malware and ransomware attacks.

- In general, e-mail filters work in two ways. First, it leverages the anti-spam techniques like keywords filtering and URL blacklisting to quarantine spam messages. The second way is to scan the malicious code in the attachments.

- E-mail filtering is just part of the protection process and no system is perfect. Users should know the threats of malware and ransomware and what to look for the signs of phishing when working with their e-mail accounts, like unrecognizable links or attachments embedded in the messages.

Advice

- Deploy e-mail filtering solutions if you maintain your own Internet e-mail gateway.

- Educate and remind staff on e-mail best practices as malware-carrying e-mails could still bypass the fixed rules of e-mail filters and deliver to users.

- Monitor for e-mail attacks and notify users timely to remove the malware-carrying e-mails that have bypassed the e-mail filters.

Source

- ITPro Portal

Newly discovered flaw undermines HTTPS connections for almost 1 000 sites

- A vulnerability was discovered in the TLS/SSL stack of F5 BIG-IP firewalls and load balancers which allows a remote attacker to extract up to 31 bytes of uninitialized memory at a time. The secret cryptographic key and other sensitive data in the memory could be leaked.

- The vulnerability affects a wide range of F5 firewalls and load balancers. From the testing results done by a security researcher, around 1 000 of the Alexa top 1 million websites were vulnerable. The memory leakage appears when the vulnerable device responds to signal acceptance of a client-supplied Session Ticket when resuming a previous TLS connection. Since each such response only exposes 31 bytes of memory data at a time, continuous requests in the logs could be observed if an attack was carried out.

- F5 has issued a patch to address the vulnerability. Exploit code is also publicly available.

Advice

- Patch the affected systems immediately.

- Monitor for any abnormal activities from firewall and load balancer logs.

- Change passwords and re-initialise cryptographic keys regularly.

Sources

- Ticketbleed
- Exploit Database
- F5
- NVD

Product Vulnerability Notes & Security Updates

1. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-February/022265.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022266.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022267.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022268.html

2. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170208-anyconnect
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170208-asa

3. **Debian**
   https://www.debian.org/security/2017/dsa-3781
   https://www.debian.org/security/2017/dsa-3782
   https://www.debian.org/security/2017/dsa-3783
   https://www.debian.org/security/2017/dsa-3784

4. **F5 Products**
   https://support.f5.com/csp/article/K43570545
   https://support.f5.com/csp/article/K73828041
   https://support.f5.com/csp/article/K00373024
   https://support.f5.com/csp/article/K05121675

5. **FortiManager**
   https://fortiguard.com/advisory/FG-IR-16-055

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201702-02
   https://security.gentoo.org/glsa/201702-03

7. **Google Android**
   https://source.android.com/security/bulletin/2017-02-01.html
   https://www.hkcert.org/my_url/en/alert/17021002

8. **Hanwha Techwin Smart Security Manager**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-040-01

9. **IBM InfoSphere Information Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg21995427

10. **ISC BIND**
    https://kb.isc.org/article/AA-01453
    https://www.hkcert.org/my_url/en/alert/17021001

11. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0040.html
    http://advisories.mageia.org/MGASA-2017-0041.html
    http://advisories.mageia.org/MGASA-2017-0042.html
    http://advisories.mageia.org/MGASA-2017-0043.html
    http://advisories.mageia.org/MGASA-2017-0044.html

12. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00003.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00004.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00005.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00014.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00015.html

13. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-0252.html
    https://linux.oracle.com/errata/ELSA-2017-0253.html
    https://linux.oracle.com/errata/ELSA-2017-0254.html
    https://linux.oracle.com/errata/ELSA-2017-3514.html
    https://linux.oracle.com/errata/ELSA-2017-3515.html
    https://linux.oracle.com/errata/ELSA-2017-3516.html

14. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:0252
    https://access.redhat.com/errata/RHSA-2017:0253
    https://access.redhat.com/errata/RHSA-2017:0254
    https://access.redhat.com/errata/RHSA-2017:0256
    https://access.redhat.com/errata/RHSA-2017:0257
    https://access.redhat.com/errata/RHSA-2017:0258
    https://access.redhat.com/errata/RHSA-2017:0259
    https://access.redhat.com/errata/RHSA-2017:0260
    https://access.redhat.com/errata/RHSA-2017:0263

15. **Sielco Sistemi Winlog SCADA Software**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-038-01

16. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170375-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170379-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170380-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170394-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170396-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170398-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170400-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170392-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170393-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170407-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170408-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170411-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170412-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170415-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170424-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170426-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170431-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170433-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170436-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170437-1.html

17. **Trend Micro Control Manager**
    https://success.trendmicro.com/solution/1116624

18. Ubuntu

https://www.ubuntu.com/usn/usn-3187-1/
https://www.ubuntu.com/usn/usn-3188-1/
https://www.ubuntu.com/usn/usn-3188-2/
https://www.ubuntu.com/usn/usn-3189-1/
https://www.ubuntu.com/usn/usn-3189-2/
https://www.ubuntu.com/usn/usn-3190-1/
https://www.ubuntu.com/usn/usn-3175-2/
https://www.ubuntu.com/usn/usn-3191-1/
https://www.ubuntu.com/usn/usn-3192-1/
https://www.ubuntu.com/usn/usn-3193-1/
https://www.ubuntu.com/usn/usn-3180-1/
https://www.ubuntu.com/usn/usn-3187-2/
https://www.ubuntu.com/usn/usn-3190-2/
https://www.ubuntu.com/usn/usn-3195-1/
https://www.ubuntu.com/usn/usn-3194-1/

Sources of product vulnerability information:

Cisco
CentOS
Debian
F5
FortiGuard
Gentoo Linux
Google Android
HKCERT
IBM
ICS-CERT
ISC BIND
Mageia
openSUSE
Oracle Linux
Red Hat
SUSE
Trend Micro
Ubuntu

Contacts:

cert@govcert.gov.hk