GovCERT.HK

Weekly IT Security News Bulletin, 2017-W11

13 March – 19 March 2017

Headlines

Check Point discloses vulnerability that allowed hackers to take over hundreds of millions of WhatsApp & Telegram accounts

- The Check Point research team has discovered a new vulnerability in both WhatsApp Web and Telegram Web. The exploitation of the vulnerability would enable attackers to control users' accounts and access the users' profiles, personal and group chats, photos, videos, contact lists, etc.

- An attacker could send an image file embedded with malicious code to a target messaging app user. Since the image file was encrypted, it could bypass checking against malicious content by the apps. A WhatsApp account would be hacked if the user just opened the image file while hacking a Telegram account required the user to further open it in a new tab. The attacker could then spread the malicious file to all of the hacked user's contacts, triggering a potential widespread attack over the two large messaging networks.

- Check Point informed WhatsApp and Telegram the security loophole on 7 March 2017. Both messaging apps vendors have verified and acknowledged the issue and produced patches for their web clients. To block malicious files, sender content is validated by the patched web clients before being encrypted.

Advice

- WhatsApp and Telegram web users should ensure that the applications are updated with the latest version and their browsers are restarted after the update.

- The users should clean "logged-in computers" regularly to control the devices that are hosting their accounts and clear unwanted activity.

- All messaging apps users are advised not to open unknown files and links from any senders.

Sources

- Check Point's blog
- Telegram's response
- Reuters' report of WhatsApp's response

U.S. charges Russian hackers for hacking millions of Yahoo email accounts

- On 15 March 2017, the Department of Justice, U.S. charges four persons for hacking activities. Some 47 crime cases were listed including conspiring to commit computer fraud and abuse, theft of trade secrets, economic espionage, wire fraud, accessing a computer without authorisation, etc.

- According to the reports, Yahoo was hacked in 2014 but the company only disclosed it two years later in September 2016, when it confirmed that more than 500 million accounts were breached. The hackers breached Yahoo's network and stole a backup copy of Yahoo's user database that contained encrypted user passwords and information which could be used to reset passwords.

- Yahoo's cookie "minting" source code was also stolen by the hackers to generate forged web browser cookies, with which the hackers could directly access at least 6,500 Yahoo accounts bypassing user authentication.

Advice

- Users are advised to change their passwords frequently and consider to enabling two-step authentication on their online services accounts, and never share use the passwords with other accounts.

- Government users shall not use private Internet email services for official communication. Business and home users should also be aware of the information security risk before exchanging sensitive or personal information with the email services.

Sources

- Department of Justice, U.S.
- The Wall Street Journal
- Wired

Product Vulnerability Notes & Security Updates

1. **Adobe Flash Player**
   https://helpx.adobe.com/security/products/flash-player/apsb17-07.html

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-March/022338.html
   https://lists.centos.org/pipermail/centos-announce/2017-March/022339.html
   https://lists.centos.org/pipermail/centos-announce/2017-March/022340.html
   https://lists.centos.org/pipermail/centos-announce/2017-March/022341.html

3. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170310-struts2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ap1800
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-wlc-mesh
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-tes
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-asr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-wsa
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-wms
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-webex
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ucs
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ucm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ucm1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ucm2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-tps
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-psc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-nss1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-nss
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-cpo
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-cpi
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-cns
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-asa

4. **Debian**
   https://www.debian.org/security/2017/dsa-3805
   https://www.debian.org/security/2017/dsa-3806
   https://www.debian.org/security/2017/dsa-3807
   https://www.debian.org/security/2017/dsa-3808
   https://www.debian.org/security/2017/dsa-3809

5. **Drupal**
   https://www.drupal.org/SA-2017-001

6. **Fatek Automation PLC Ethernet Module**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-073-01

7. **F5 Products**
   https://support.f5.com/csp/article/K55001100

8. **Huawei Products**
   http://www.huawei.com/en/psirt/security-notices/huawei-sn-20170313-01-struts2-en

9. **IBM WebSphere Application Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg21999293
   http://www-01.ibm.com/support/docview.wss?uid=swg22000172
   https://www.auscert.org.au/render.html?it=45146

10. **LAquis SCADA software**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-075-01

11. **Linux kernel**
   https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.10.3
   https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2636

12. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0073.html
   http://advisories.mageia.org/MGASA-2017-0074.html
   http://advisories.mageia.org/MGASA-2017-0075.html
   http://advisories.mageia.org/MGASA-2017-0076.html

13. **Microsoft Products**
   https://technet.microsoft.com/library/security/ms17-mar
   https://technet.microsoft.com/en-us/library/security/MS17-006
   https://technet.microsoft.com/en-us/library/security/MS17-007
   https://technet.microsoft.com/en-us/library/security/MS17-008
   https://technet.microsoft.com/en-us/library/security/MS17-009
   https://technet.microsoft.com/en-us/library/security/MS17-010
   https://technet.microsoft.com/en-us/library/security/MS17-011
   https://technet.microsoft.com/en-us/library/security/MS17-012
   https://technet.microsoft.com/en-us/library/security/MS17-013
   https://technet.microsoft.com/en-us/library/security/MS17-014
   https://technet.microsoft.com/en-us/library/security/MS17-015
   https://technet.microsoft.com/en-us/library/security/MS17-016
   https://technet.microsoft.com/en-us/library/security/MS17-017
   https://technet.microsoft.com/en-us/library/security/MS17-018
   https://technet.microsoft.com/en-us/library/security/MS17-019
   https://technet.microsoft.com/en-us/library/security/MS17-020
   https://technet.microsoft.com/en-us/library/security/MS17-021
   https://technet.microsoft.com/en-us/library/security/MS17-022
   https://technet.microsoft.com/en-us/library/security/MS17-023

14. **OpenSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-03/msg00008.html
   https://lists.opensuse.org/opensuse-security-announce/2017-03/msg00009.html
   https://lists.opensuse.org/opensuse-security-announce/2017-03/msg00011.html

15. **Oracle Linux**
   https://linux.oracle.com/errata/ELSA-2017-0498.html
   https://linux.oracle.com/errata/ELSA-2017-0527.html

16. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:0501
    https://access.redhat.com/errata/RHSA-2017:0515
    https://access.redhat.com/errata/RHSA-2017:0526
    https://access.redhat.com/errata/RHSA-2017:0527
    https://access.redhat.com/errata/RHSA-2017:0530
    https://access.redhat.com/errata/RHSA-2017:0531
    https://access.redhat.com/errata/RHSA-2017:0532
    https://access.redhat.com/errata/RHSA-2017:0533
    https://access.redhat.com/errata/RHSA-2017:0535
    https://access.redhat.com/errata/RHSA-2017:0536
    https://access.redhat.com/errata/RHSA-2017:0549

17. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.539975

18. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170656-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170661-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170694-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170695-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170696-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170701-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170702-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170703-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170704-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170705-1.html

19. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3226-1/
    https://www.ubuntu.com/usn/usn-3227-1/
    https://www.ubuntu.com/usn/usn-3228-1/
    https://www.ubuntu.com/usn/usn-3229-1/
    https://www.ubuntu.com/usn/usn-3230-1/
    https://www.ubuntu.com/usn/usn-3231-1/
    https://www.ubuntu.com/usn/usn-3232-1/
    https://www.ubuntu.com/usn/usn-3234-1/
    https://www.ubuntu.com/usn/usn-3234-2/
    https://www.ubuntu.com/usn/usn-3235-1/

20. **VMware Products**
    http://www.vmware.com/security/advisories/VMSA-2017-0004.html
    http://www.vmware.com/security/advisories/VMSA-2017-0005.html

21. **Xen**
    http://xenbits.xen.org/xsa/advisory-211.html

Sources of product vulnerability information:

- Adobe
- CentOS
- Cisco
- Debian
- Drupal
- F5
- Huawei
- IBM
- ICS-CERT
- Linux Kernel Organization
- Mageia
- Microsoft
- NIST-NVD
- OpenSUSE
- Oracle Linux
- RedHat
- Slackware
- SUSE
- Ubuntu
- VMware
- Xen

Contacts:

cert@govcert.gov.hk