GovCERT.HK

Weekly IT Security News Bulletin, 2017-W14

3 April 2017 – 9 April 2017

Headlines

iCloud mail phishing scam wants to steal Apple accounts, banking data, identity

- There is a phishing campaign intended to steal Apple users' information. A fake "Welcome to iCloud" email with subject like "Dear Customer, We are unable to confirm your account information" cheats the users to click the given link to resume the claimed suspended iCloud services.
- The link leads to a phishing website imitating the real Apple ID sign-in page to collect the user's Apple ID, password, name, credit card details, home address, phone number and date of birth. Once finished, the user will be redirected to a genuine Apple website.
- The scammers could then impersonate the victims to access their Apple accounts, all contents such as private photos stored in the iCloud, shop online using their credit cards, and send further phishing emails in the victims' names.

Advice

- Do not follow URL links from un-trusted or un-checked sources to avoid being re-directed to malicious or phishing websites.
- Log in only at self-typed or bookmarked official website addresses.
- Verify that your browser is securely connected to the official websites presenting valid server certificates.
- Turn-on two-factor authentication for your Apple ID to strengthen the security of your user account.

Sources

- Hoax-Slayer
- Softpedia
- Apple Inc.

Smartphones using Broadcom Wi-Fi chip can be hacked over-the-air

- The Broadcom Wi-Fi System-on-Chip (SoC) widely used in Android and iOS devices is found vulnerable to remote code execution over the air by hackers on the same Wi-Fi network of the targeted devices.

- A Google Project Zero researcher proved the vulnerability by sending specially crafted Wi-Fi frames to the Wi-Fi SoC, causing stack overflow, enabling subsequent code execution. The researcher commented that Broadcom lacked some basic security measures on its Wi-Fi firmware implementation including stack cookies, safe unlinking, and access permission protection.

- Smartphones including Google's Nexus 5, 6 and 6P, most high-end Samsung phones and all Apple iPhone 4 and later are vulnerable. Apple iOS 10.3.1 was released to fix the vulnerability for iPhone 5 or later while Google Nexus and Pixel phones could be fixed by the Android security patch for April 2017. Other Android users have to wait for patches released by the other manufacturers. Some smartphones, like iPhone 4 or older Android phones may never be patched.

Advice

- Install the latest iOS or Android versions available on your mobile devices.

- Disable Wi-Fi when not on a known and trusted network.

- Instruct the phone to forget any saved Wi-Fi network that is not a private, secured known network to avoid automatically connected to a risky network.

- Avoid using de-supported mobile devices, which vulnerabilities may no longer be patched.

Sources

- Google Project Zero
- Google Android Security Bulletin
- Apple Security Updates
- NIST NVD (CVE-2017-0561, CVE-2017-6957)
- Yahoo Tech

Microsoft Office zero-day attacks through OLE

- McAfee revealed a zero-day vulnerability of the Windows Object Linking and Embedding (OLE) in Microsoft Office after analyzing a malicious Word document. The malicious Word document is embedded with an OLE link object pointing to an HTML Application (HTA) file. Once the document is opened, the HTA file will be downloaded and run with its scripts for any malicious activities on the victim's computer, without user interaction.

- OLE is wildly adopted in Microsoft Office documents to dynamically incorporate different kinds of data from different sources. The OLE vulnerability could therefore affect all Microsoft Office products, including the latest Office 2016 running on Windows 10.

- Both McAfee and FireEye published articles about the issue. McAfee tested that the attack would not be triggered if the Microsoft Office Protected View is enabled. The attack is being exploited in wild and the earliest attack was observed since the late January 2017. So far Microsoft has not responded to the issue.

Advice

- Do not open any Microsoft Office documents from untrusted sources.

- Enable Protected View in Microsoft Office products.

- Update Microsoft Office products with latest patches once available.

- Remove admin rights from user accounts to contain attack impacts.

Sources

- McAfee Labs
- FireEye Threat Research Blog
- Microsoft - Enable Protected View in Microsoft Office

Product Vulnerability Notes & Security Updates

1. **Apple iOS**
   https://support.apple.com/zh-hk/HT207688

2. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-aironet
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ame
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-asr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cfpw
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cfpw1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cimc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cli
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cli1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cli2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cme
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cpi
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ios
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-iosxe
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-res
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucm1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucs
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucs-director
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucs1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc3

3. **Debian**
   https://www.debian.org/security/2017/dsa-3825
   https://www.debian.org/security/2017/dsa-3826

4. **F5 products**
   https://support.f5.com/csp/article/K26311635

5. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0095.html
   http://advisories.mageia.org/MGASA-2017-0096.html
   http://advisories.mageia.org/MGASA-2017-0097.html
   http://advisories.mageia.org/MGASA-2017-0098.html
   http://advisories.mageia.org/MGASA-2017-0099.html
   http://advisories.mageia.org/MGASA-2017-0100.html
   http://advisories.mageia.org/MGASA-2017-0101.html
   http://advisories.mageia.org/MGASA-2017-0102.html
   http://advisories.mageia.org/MGASA-2017-0103.html
   http://advisories.mageia.org/MGASA-2017-0104.html
   http://advisories.mageia.org/MGASA-2017-0105.html

6. **OpenSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00000.html
   https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00001.html
   https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00002.html
   https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00003.html
   https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00007.html
   https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00008.html
   https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00009.html

7. **Oracle Linux**
   https://linux.oracle.com/errata/ELSA-2017-3533.html
   https://linux.oracle.com/errata/ELSA-2017-3534.html
   https://linux.oracle.com/errata/ELSA-2017-3535.html

8. **Red Hat**
   https://access.redhat.com/errata/RHSA-2017:0847
   https://access.redhat.com/errata/RHSA-2017:0854
   https://access.redhat.com/errata/RHSA-2017:0855
   https://access.redhat.com/errata/RHSA-2017:0860
   https://access.redhat.com/errata/RHSA-2017:0861
   https://access.redhat.com/errata/RHSA-2017:0862
   https://access.redhat.com/errata/RHSA-2017:0863
   https://access.redhat.com/errata/RHSA-2017:0864
   https://access.redhat.com/errata/RHSA-2017:0867
   https://access.redhat.com/errata/RHSA-2017:0869
   https://access.redhat.com/errata/RHSA-2017:0872
   https://access.redhat.com/errata/RHSA-2017:0873
   https://access.redhat.com/errata/RHSA-2017:0879
   https://access.redhat.com/errata/RHSA-2017:0880
   https://access.redhat.com/errata/RHSA-2017:0881
   https://access.redhat.com/errata/RHSA-2017:0882

9. **Rockwell Automation Products**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-094-03

10. **Schneider Electric Wonderware InTouch Access Anywhere**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-089-01
    https://ics-cert.us-cert.gov/advisories/ICSA-17-089-02

11. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.427595

12. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170899-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170901-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170912-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170913-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170914-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170918-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170940-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170945-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170946-1.html

https://www.suse.com/support/update/announcement/2017/suse-su-20170948-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170950-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170951-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170953-1.html

13. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3253-1/
    https://www.ubuntu.com/usn/usn-3254-1/
    https://www.ubuntu.com/usn/usn-3255-1/
    https://www.ubuntu.com/usn/usn-3256-1/
    https://www.ubuntu.com/usn/usn-3256-2/

14. **Xen**
    http://xenbits.xen.org/xsa/advisory-212.html

Sources of product vulnerability information:

Apple
Cisco
Debian
F5
ICS-CERT
Mageia
OpenSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
Xen

Contacts:

cert@govcert.gov.hk