GovCERT.HK

Weekly IT Security News Bulletin, 2017-W16

17 April 2017 – 23 April 2017

Headlines

BrickerBot permanent denial-of-service attack

- The "BrickerBot" attack is a hardware-damaging assault targeting on Internet of Things (IoT) devices. It exploits the devices' hard-coded passwords to destroy the firmware and/or basic function of the systems, causing permanent denial of service (PDoS), or so-called "phlashing".
- The Bot launches brute force attacks at the open Telnet port of the device, using the username/password pair 'root/vizxv' as its first attempt. Upon successful login, a series of Linux commands are performed to corrupt the device storage, disrupt Internet connectivity and device performance, and wipe all files on the device.
- A security product vendor's honeypot logged 1,895 PDoS attempts performed from several locations around the world over a four-day period starting from 20 March 2017. The origins of the attack included a limited number of IP addresses around the world and were identified as network devices including wireless access points and bridges exposing their SSH port and running an older version of SSH server.

Advice

- Disable Telnet access from the Internet to IoT devices.
- Remove all unnecessary network services, protocols and applications from devices.
- Change the factory-default username and password of devices.
- Implement host and/or network-based intrusion detection and prevention systems to block unnecessary connections and operations.

Sources

- ICS-CERT
- Radware
- Trend Micro

When flashlights attack, Android passwords get stolen

- The malware called "Flashlight LED Widget" has masqueraded as a flashlight app on Google Play for download since 10 March 2017. There were up to 5,000 downloads until the malicious app was removed from the store on 10 April 2017.

- The malware can infect all Android versions to steal the victim's credit card details or banking app credentials. It evades Google's detection of its malicious functionality by encrypting its payload in the APK file. Once installed, the app requests device administrator rights, registers the device to the attacker's server, sends out the device information, a list of installed applications and even a picture of the device owner taken by the device camera.

- Based on the installed applications, the server sends the corresponding malicious HTML code to run fake activity overlaying what the victim launches, such as Facebook, WhatsApp, Instagram, Google Play, and mobile banking apps. The victim's device will also be locked remotely with a fake update screen to hide fraudulent activity such as cashing out the compromised bank accounts.

Advice

- Download and install apps only from official sources.

- Review permissions requested before installing apps.

- Install an anti-malware app on Android devices and keep it up-to-date.

Sources

- ESET
- SC Magazine

Product Vulnerability Notes & Security Updates

1. **CentOS**

https://lists.centos.org/pipermail/centos-announce/2017-April/022359.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022370.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022376.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022380.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022384.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022386.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022387.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022390.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022391.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022392.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022393.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022394.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022395.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022396.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022397.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022398.html
https://lists.centos.org/pipermail/centos-announce/2017-April/022399.html

2. **Cisco Products**

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-dns
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-norm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-ipsec
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-tls
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-xauth
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cpi
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-energywise
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-findit
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-fpsnort
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-ios-xe-snmp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-prime-dns
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-ucm

3. **Debian**

https://www.debian.org/security/2017/dsa-3830
https://www.debian.org/security/2017/dsa-3831

4. **Drupal 8**

https://www.drupal.org/SA-CORE-2017-002

5. **F5 Products**
   https://support.f5.com/csp/article/K60104355
   https://support.f5.com/csp/article/K71877858

6. **Google Chrome**
   https://chromereleases.googleblog.com/2017/04/stable-channel-update-for-desktop.html

7. **Huawei Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170419-01-openssl-en
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170419-01-pse-en
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170420-01-fusionsphere-en

8. **IBM Domino and WebSphere Application Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg21996847
   http://www-01.ibm.com/support/docview.wss?uid=swg22002280

9. **Juniper Products**
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10776
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10777
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10778
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10780
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10784
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10785
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10786

10. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0106.html
    http://advisories.mageia.org/MGASA-2017-0107.html
    http://advisories.mageia.org/MGASA-2017-0108.html
    http://advisories.mageia.org/MGASA-2017-0109.html
    http://advisories.mageia.org/MGASA-2017-0110.html

11. **Mozilla Firefox**
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-10/
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-11/
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-12/

12. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00017.html
    https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00018.html
    https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00019.html
    https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00022.html
    https://lists.opensuse.org/opensuse-security-announce/2017-04/msg00025.html

13. **Oracle Products**
    http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html

14. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-3537.html
    https://linux.oracle.com/errata/ELSA-2017-3538.html
    https://linux.oracle.com/errata/ELSA-2017-3539.html
    https://linux.oracle.com/errata/ELSA-2017-0933-1.html
    https://linux.oracle.com/errata/ELSA-2017-0979.html

https://linux.oracle.com/errata/ELSA-2017-0987.html
https://linux.oracle.com/errata/ELSA-2017-1095.html
https://linux.oracle.com/errata/ELSA-2017-1100.html
https://linux.oracle.com/errata/ELSA-2017-1104.html
https://linux.oracle.com/errata/ELSA-2017-1105.html
https://linux.oracle.com/errata/ELSA-2017-1106.html
https://linux.oracle.com/errata/ELSA-2017-1108.html
https://linux.oracle.com/errata/ELSA-2017-1109.html

15. Red Hat

https://access.redhat.com/errata/RHSA-2017:1095
https://access.redhat.com/errata/RHSA-2017:1101
https://access.redhat.com/errata/RHSA-2017:1102
https://access.redhat.com/errata/RHSA-2017:1103

16. Schneider Electric Modicon M221 PLCs and SoMachine Basic

https://ics-cert.us-cert.gov/advisories/ICSA-17-103-02

17. Slackware

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.553873

18. SUSE

https://www.suse.com/support/update/announcement/2017/suse-su-20170998-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170999-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171000-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171003-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171004-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171010-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171012-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171027-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171030-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171039-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171040-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171041-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171042-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171043-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171044-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171047-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171048-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171052-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171058-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171059-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171060-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171062-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171064-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171065-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171067-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171080-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171081-1.html

19. Trend Micro Products

https://success.trendmicro.com/solution/1117192

20. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3259-1/
    https://www.ubuntu.com/usn/usn-3261-1/
    https://www.ubuntu.com/usn/usn-3262-1/

21. **Wecon Technologies LEVI Studio HMI Editor**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-103-01

22. **VMWare Products**
    http://www.vmware.com/security/advisories/VMSA-2017-0007.html
    http://www.vmware.com/security/advisories/VMSA-2017-0008.html

23. **Wireshark**
    https://www.wireshark.org/security/wnpa-sec-2017-12.html
    https://www.wireshark.org/security/wnpa-sec-2017-13.html
    https://www.wireshark.org/security/wnpa-sec-2017-14.html
    https://www.wireshark.org/security/wnpa-sec-2017-15.html
    https://www.wireshark.org/security/wnpa-sec-2017-16.html
    https://www.wireshark.org/security/wnpa-sec-2017-17.html
    https://www.wireshark.org/security/wnpa-sec-2017-18.html
    https://www.wireshark.org/security/wnpa-sec-2017-19.html
    https://www.wireshark.org/security/wnpa-sec-2017-20.html
    https://www.wireshark.org/security/wnpa-sec-2017-21.html

Sources of product vulnerability information:

CentOS
Cisco
Debian
Drupal
F5
Google Chrome
Huawei
IBM
ICS-CERT
Juniper
Mageia
Mozilla Firefox
openSUSE
Oracle
Oracle Linux
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
VMWare
Wireshark

Contacts:

cert@govcert.gov.hk