GovCERT.HK

Weekly IT Security News Bulletin, 2017-W7

13 February – 19 February 2017

Headlines

Analysis of Internet-connected devices reveals millions are vulnerable to attack

- Shodan is a search engine for Internet connected devices and systems around the world, such as webcams, baby monitors, medical equipment, industrial control system devices, home appliances, databases and others. Shodan provides not only the IP address of the device but also other useful information for attackers such as its product name, firmware version, operating system, application software and opened ports and so on.

- Based on data from Shodan, a security vendor revealed that millions of unsecured devices were exposed to the Internet in a research study focused on large U.S. cities. Many of the exposed devices were found vulnerable to exploitation and compromise.

- The exposed devices could be leaking sensitive or personal data without the device owners' knowledge. The compromised devices could be the entry point into a corporate infrastructure for lateral movement and further attacks. They could also be turned into part of botnets for attackers to launch attacks to third parties.

Advice

- Review configurations of Internet-connected devices and ensure that all unnecessary ports and services are disabled.

- Change default access passwords or disable default login accounts

- Apply latest patches or upgrade to the latest firmware versions for Internet-connected devices.

Sources

- Trend Micro
- Shodan

Yahoo warns users of account breaches related to recent attacks

- Yahoo announced that around 32 million of their user accounts were accessed by attackers in 2015 and 2016 using a forge cookie attack. The company believed an unauthorised attacker accessed the company's proprietary code to learn how to forge the cookies and stolen millions of user information, such as names, email addresses, hashed passwords, telephone numbers, dates of birth, and, in some cases, encrypted or unencrypted security questions and answers.

- Yahoo recommended users to review their accounts for anomaly and be cautious of unsolicited communications asking for personal information and avoid clicking hyperlinks or downloading attachments from suspicious emails.

Advice

- Change the password and review the activity logs of your account regularly.

- Do not store government classified or sensitive information on private webmail services.

Sources

- Yahoo
- Computer World

Product Vulnerability Notes & Security Updates

1. **Adobe Flash Player**
   https://helpx.adobe.com/security/products/flash-player/apsb17-04.html

2. **Advantech WebAccess Server**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-045-01

3. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-February/022269.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022270.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022271.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022272.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022273.html

4. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-asyncos
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cms
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cms1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cucm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cucm1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cucm2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cucm3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-fpmc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-idm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ise
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-pcp1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-pcp2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-pcp3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ucm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ucs

5. **Debian**
   https://www.debian.org/security/2017/dsa-3785
   https://www.debian.org/security/2017/dsa-3786
   https://www.debian.org/security/2017/dsa-3787
   https://www.debian.org/security/2017/dsa-3788
   https://www.debian.org/security/2017/dsa-3789

6. **F5 Products**
   https://support.f5.com/csp/article/K12685114
   https://support.f5.com/csp/article/K08383757
   https://support.f5.com/csp/article/K31336596
   https://support.f5.com/csp/article/K50459349
   https://support.f5.com/csp/article/K59836191
   https://support.f5.com/csp/article/K73926196
   https://support.f5.com/csp/article/K44512851

7. **Gentoo Linux**
   https://security.gentoo.org/glsa/201702-04
   https://security.gentoo.org/glsa/201702-05
   https://security.gentoo.org/glsa/201702-06
   https://security.gentoo.org/glsa/201702-07
   https://security.gentoo.org/glsa/201702-08

8. **Geutebrück IP Cameras**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-045-02

9. **IBM WebSphere Application Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg21997743

10. **IBM WebSphere Remote Server**
    http://www.ibm.com/support/docview.wss?uid=swg21998689

11. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0045.html
    http://advisories.mageia.org/MGASA-2017-0046.html
    http://advisories.mageia.org/MGASA-2017-0047.html

12. **OpenSSL**
    https://www.openssl.org/news/secadv/20170216.txt

13. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00020.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00021.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00022.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00026.html
    https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00027.html

14. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-0269.html
    https://linux.oracle.com/errata/ELBA-2017-0274.html
    https://linux.oracle.com/errata/ELSA-2017-0276.html

15. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:0269
    https://access.redhat.com/errata/RHSA-2017:0270
    https://access.redhat.com/errata/RHSA-2017:0275
    https://access.redhat.com/errata/RHSA-2017:0276
    https://access.redhat.com/errata/RHSA-2017:0282

16. **Siemens SIMATIC Products**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-045-03

17. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170441-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170453-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170459-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170460-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170461-1.html

https://www.suse.com/support/update/announcement/2017/suse-su-20170464-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170470-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170471-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170473-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20170474-1.html

18. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3196-1/
    https://www.ubuntu.com/usn/usn-3197-1/
    https://www.ubuntu.com/usn/usn-3198-1/
    https://www.ubuntu.com/usn/usn-3199-1/
    https://www.ubuntu.com/usn/usn-3200-1/
    https://www.ubuntu.com/usn/usn-3201-1/

19. **Xen**
    http://xenbits.xen.org/xsa/advisory-208.html

Sources of product vulnerability information:

Adobe
Cisco
CentOS
Debian
F5
Gentoo Linux
IBM
ICS-CERT
Mageia
OpenSSL
openSUSE
Oracle Linux
Red Hat
SUSE
Ubuntu
Xen

Contacts:

cert@govcert.gov.hk