GovCERT.HK

Weekly IT Security News Bulletin, 2017-W35

28 August – 3 September 2017

Headlines

Over thousands internet-connected devices left wide open to hackers

- A list of more than 8,200 unique IP addresses, together with associated credentials, were leaked online affecting thousands of Internet-connected devices. The list has been posted on an Internet-facing website since June 2017 and recorded over 13,000 view counts.

- Having examined by some security analysts, near 2,200 IP addresses were reachable via remote telnet access port. Worst of all, about 1,800 credentials for these telnet-accessible IP addresses were still functional. The analysts also observed that users continued to apply common and even default password for their devices. When kept monitoring the list, it was believed some devices had already been infected with botnets as some devices' username-password combinations were changed to those commonly used by botnets since first identified.

- There were precedent cyber attacks involving malwares able to guess administration credentials and intrude into devices through telnet. Mirai and BrickerBot uncovered in 2016 and 2017 respectively utilised the same tactics to launch denial-of-service (DoS) attacks. The former turns devices into botnets to initiate massive distributed DoS attacks to incapacitate victims, while the latter permanently renders infected devices inoperable.

Advice

- Disable unnecessary features and services, such as telnet and remote management, on your Internet-connected devices.

- Deploy devices behind Internet firewall or router and block telnet access port from the Internet if not necessary.

- Change the default credentials and set strong passwords for devices.

Sources

- Ars Technica
- Infosecurity Magazine
- Security Affairs

瀏覽器防護機制存漏洞 擴充程式可被黑客利用

- 研究人員在八月初舉行的 USENIX 資訊保安研討會上揭露了兩種瀏覽器防護機制的漏洞。透過利用這些漏洞，惡意網頁可以獲取使用者瀏覽器上的擴充程式列表，甚至避開瀏覽器的接達控制，使瀏覽器上擴充程式的資源在未經授權下被存取。

- 第一種漏洞主要針對包括以 Chromium 為核心的瀏覽器（如 Chrome、Opera 等）或 Firefox 瀏覽器。一般情況下，瀏覽器在網頁嘗試存取擴充程式的資源時，瀏覽器會先確認該擴充程式是否已經安裝，然後檢查其資源是否可予以網站使用。研究發現瀏覽器在核實擴充程式的資源請求時，對真正和無效請求所需要的時間會有所不同，攻擊者因此可利用該時間差距，準確推算出所有已安裝在使用者瀏覽器上的擴充程式。

- 第二種漏洞針對 Safari 瀏覽器。在正常情況下，每當開啟瀏覽器程式時，每個擴充程式都會被分配一組隨機統一資源標誌符（即 Uniform Resource Identifier，URI），而且每組 URI 通常只有相對應的擴充程式能夠讀取，籍以保護擴充程式的資源。但研究指出，這種防護機制容易令擴充程式的開發者錯誤地曝露其 URI，使網頁和其他擴充程式可透過其 URI 接達其資源。

- 透過以上瀏覽器的漏洞，攻擊者不但可以識別個別用戶和收集用戶的瀏覽習慣，還可以利用擴充程式中的保安漏洞進行針對性的惡意攻擊，例如：竊取敏感資料等。至今仍未有瀏覽器廠商為漏洞提供修補程式。

Advice

- 移除無必要使用的擴充程式，並定期更新瀏覽器到最新版本。

- 不要開啟來歷不明的電郵中的超連結或附件。

- 避免在瀏覽器的擴充程式中儲存或處理敏感資料。

Sources

- iThome
- Bleeping Computer
- Security Week
- USENIX

Product Vulnerability Notes & Security Updates

1. **Abbott Laboratories' Products**
   https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01

2. **Advantech WebAccess**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-241-02

3. **AzeoTech DAQFactory**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-241-01

4. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-August/022527.html
   https://lists.centos.org/pipermail/centos-announce/2017-August/022529.html

5. **Debian**
   https://www.debian.org/security/2017/dsa-3954
   https://www.debian.org/security/2017/dsa-3955
   https://www.debian.org/security/2017/dsa-3956
   https://www.debian.org/security/2017/dsa-3957
   https://www.debian.org/security/2017/dsa-3958
   https://www.debian.org/security/2017/dsa-3959

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201708-09
   https://security.gentoo.org/glsa/201708-10

7. **Huawei FusionSphere OpenStack**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170830-01-OpenStack-en
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170830-02-OpenStack-en

8. **IBM Products**
   http://www-01.ibm.com/support/docview.wss?uid=swg21997877
   http://www-01.ibm.com/support/docview.wss?uid=swg21999384
   http://www-01.ibm.com/support/docview.wss?uid=swg21999385
   http://www-01.ibm.com/support/docview.wss?uid=swg22002676
   http://www-01.ibm.com/support/docview.wss?uid=swg22006996
   http://www-01.ibm.com/support/docview.wss?uid=swg22007002

9. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0307.html
   http://advisories.mageia.org/MGASA-2017-0308.html
   http://advisories.mageia.org/MGASA-2017-0309.html
   http://advisories.mageia.org/MGASA-2017-0310.html
   http://advisories.mageia.org/MGASA-2017-0311.html
   http://advisories.mageia.org/MGASA-2017-0312.html
   http://advisories.mageia.org/MGASA-2017-0313.html
   http://advisories.mageia.org/MGASA-2017-0314.html
   http://advisories.mageia.org/MGASA-2017-0315.html
   http://advisories.mageia.org/MGASA-2017-0316.html
   http://advisories.mageia.org/MGASA-2017-0317.html
   http://advisories.mageia.org/MGASA-2017-0318.html

http://advisories.mageia.org/MGASA-2017-0319.html
http://advisories.mageia.org/MGASA-2017-0320.html

10. **Moxa SoftCMS Live Viewer**
https://ics-cert.us-cert.gov/advisories/ICSA-17-243-05

11. **openSUSE**
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00067.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00068.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00072.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00076.html
https://lists.opensuse.org/opensuse-security-announce/2017-08/msg00077.html

12. **OPW Fuel Management Systems**
https://ics-cert.us-cert.gov/advisories/ICSA-17-243-04

13. **Oracle Linux**
https://linux.oracle.com/errata/ELSA-2017-2550.html
https://linux.oracle.com/errata/ELSA-2017-2551.html
https://linux.oracle.com/errata/ELSA-2017-2563.html

14. **Red Hat**
https://access.redhat.com/errata/RHSA-2017:2553
https://access.redhat.com/errata/RHSA-2017:2557
https://access.redhat.com/errata/RHSA-2017:2560
https://access.redhat.com/errata/RHSA-2017:2563

15. **Siemens Products**
https://ics-cert.us-cert.gov/advisories/ICSA-17-243-01
https://ics-cert.us-cert.gov/advisories/ICSA-17-243-02

16. **SUSE**
https://www.suse.com/support/update/announcement/2017/suse-su-20172257-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172258-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172263-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172264-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172266-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172267-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172280-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172281-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172286-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172290-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172293-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172294-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172299-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172300-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172302-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172303-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172312-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172315-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172317-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172318-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172319-1.html

https://www.suse.com/support/update/announcement/2017/suse-su-20172320-1.html

17. **Symantec ProxyClient for Windows**
    https://www.symantec.com/security-center/network-protection-security-advisories/SA152

18. **Ubuntu**
    https://usn.ubuntu.com/usn/usn-3199-3/
    https://usn.ubuntu.com/usn/usn-3403-1/
    https://usn.ubuntu.com/usn/usn-3404-1/
    https://usn.ubuntu.com/usn/usn-3404-2/
    https://usn.ubuntu.com/usn/usn-3405-1/
    https://usn.ubuntu.com/usn/usn-3405-2/
    https://usn.ubuntu.com/usn/usn-3406-1/
    https://usn.ubuntu.com/usn/usn-3406-2/
    https://usn.ubuntu.com/usn/usn-3407-1/

19. **Wireshark**
    https://www.wireshark.org/security/wnpa-sec-2017-38.html
    https://www.wireshark.org/security/wnpa-sec-2017-39.html
    https://www.wireshark.org/security/wnpa-sec-2017-40.html
    https://www.wireshark.org/security/wnpa-sec-2017-41.html

Sources of product vulnerability information:

CentOS
Debian
IBM
Gentoo Linux
Huawei
ICS-CERT
Mageia
openSUSE
Oracle Linux
Red Hat
SUSE
Symantec
Ubuntu
Wireshark

Contacts:

cert@govcert.gov.hk