GovCERT.HK

Weekly IT Security News Bulletin, 2017-W41

9 October – 15 October 2017

Headlines

New smart speaker found eavesdropping everything

- Google Home Mini is a newly released smart speaker enabling users to interact with Google's services with voice commands. A reporter reviewing the product found that it recorded all sound and sent the recordings to Google's servers automatically without user instructions. It may lead to privacy concerns about such devices eavesdropping on users' private conversations. The vendor admitted that the flaw happened in some of its early batch of released devices.

- The device is by design activated only when hearing the wake phrase "OK Google" or "Hey Google", or when being long pressed at the top. The vendor explained that an issue impacting a small number of the devices could cause the touch control mechanism to behave incorrectly.

- The vendor rolled out a software update on 7 October 2017 to fix the issue. In addition, it has decided to remove all touch panel functionality to avoid any confusion and give its users complete peace of mind, through another software update by 15 October 2017. It has also erased any audio clips, activities and queries that were created by long pressing the top of the device.

Advice

- Keep firmware, operating system and applications of your Internet-connected devices up-to-date.

- Turn off or disable services that are not necessary at your devices.

- Read the privacy policy and be aware of what data would be collected and sent out from the devices.

Sources

- Google Home Support
- Android Police
- The Verge
- The Telegraph

Cryptojacking consumes your computer to make money

- Cryptocurrencies, such as Bitcoin and Monero, are digital money safe-keeping all transaction records on a distributed public ledger with cryptographic technologies. Their "coins" are generated through a process called "mining", which uses computer power to solve complicated maths problems to verify and process the cryptocurrency transactions that other people announce. Cryptojacking is the malicious act to silently plant coin-mining JavaScript on web pages for running on web browsers so that miscreants could "steal" visitors' computer resources to generate revenue.

- The JavaScript libraries for mining cryptocurrency are provided by legitimate service providers. Coinhive is the first one providing in-browser miner scripts that website owners can load on their sites to mine Monero using their visitors' computing power. It advertises its service as an alternative to classic ads and advises the website owners to warn their visitors when the script is loaded. Since Coinhive's service launch on 14 September 2017, three new players offering the same service, including JSEcoin, CryptoLoot and MineMyTraffic have emerged.

- Some website owners however deploy the miner service without letting visitors know, getting their approvals, or providing ways to opt out. Malware authors have also joined the Coinhive abuses by secretly embedding the Coinhive library in Chrome extensions, typosquatted domains, malvertising campaigns and even an online game modding platform.

Advice

- Keep your anti-malware engines and signatures up-to-date to block malicious scripts or programs carrying out uninformed coin-mining activities.

- Deploy ad blockers or miner blockers on web browsers, which could stop the coin-mining scripts from executing at the browser level.

- Block domains of the miner service providers at the network level to protect your organisation's computers from accessing the miner scripts.

Sources

- Bleeping Computer: 23 September, 10 October, 11 October
- ADGUARD
- The Telegraph

Product Vulnerability Notes & Security Updates

1. **Apple iOS**
   https://support.apple.com/kb/HT208182

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-October/022563.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022564.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022565.html

3. **Debian**
   https://www.debian.org/security/2017/dsa-3992
   https://www.debian.org/security/2017/dsa-3993
   https://www.debian.org/security/2017/dsa-3994
   https://www.debian.org/security/2017/dsa-3995
   https://www.debian.org/security/2017/dsa-3996
   https://www.debian.org/security/2017/dsa-3997
   https://www.debian.org/security/2017/dsa-3998

4. **Envitech Ltd. EnviDAS Ultimate**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-285-03

5. **F5 Products**
   https://support.f5.com/csp/article/K11936401
   https://support.f5.com/csp/article/K41815723
   https://support.f5.com/csp/article/K52342540
   https://support.f5.com/csp/article/K91024405

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201710-01
   https://security.gentoo.org/glsa/201710-02
   https://security.gentoo.org/glsa/201710-03
   https://security.gentoo.org/glsa/201710-04
   https://security.gentoo.org/glsa/201710-05
   https://security.gentoo.org/glsa/201710-06
   https://security.gentoo.org/glsa/201710-07
   https://security.gentoo.org/glsa/201710-08
   https://security.gentoo.org/glsa/201710-09

7. **IBM Products**
   http://www-01.ibm.com/support/docview.wss?uid=swg22004066
   http://www-01.ibm.com/support/docview.wss?uid=swg22006815

8. **JanTek JTC-200**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-283-02

9. **Juniper Products**
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10807
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10809
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10810
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10811
   https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10813

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10814
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10816
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10817

10. **LAVA Computer MFG Inc. Ether-Serial Link**
https://ics-cert.us-cert.gov/advisories/ICSA-17-283-01

11. **Mageia**
http://advisories.mageia.org/MGASA-2017-0362.html
http://advisories.mageia.org/MGASA-2017-0363.html
http://advisories.mageia.org/MGASA-2017-0364.html
http://advisories.mageia.org/MGASA-2017-0365.html
http://advisories.mageia.org/MGASA-2017-0366.html
http://advisories.mageia.org/MGASA-2017-0367.html

12. **Microsoft Products**
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/313ae481-3088-e711-80e2-000d3a32fc99
https://support.microsoft.com/en-us/help/20171010/security-update-for-vulnerabilities-in-windows-server-2008
https://www.hkcert.org/my_url/en/alert/17101101

13. **NXP Semiconductors MQX RTOS**
https://ics-cert.us-cert.gov/advisories/ICSA-17-285-04

14. **Oracle Linux**
https://linux.oracle.com/errata/ELSA-2017-2801.html
https://linux.oracle.com/errata/ELSA-2017-2863.html
https://linux.oracle.com/errata/ELSA-2017-2882.html
https://linux.oracle.com/errata/ELSA-2017-3629.html

15. **ProMinent MultiFLEX M10a Controller**
https://ics-cert.us-cert.gov/advisories/ICSA-17-285-01

16. **Red Hat**
https://access.redhat.com/errata/RHSA-2017:2869
https://access.redhat.com/errata/RHSA-2017:2882
https://access.redhat.com/errata/RHSA-2017:2886
https://access.redhat.com/errata/RHSA-2017:2888
https://access.redhat.com/errata/RHSA-2017:2889

17. **Slackware**
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.395569
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.419253
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.872751

18. **Siemens BACnet Field Panels**
https://ics-cert.us-cert.gov/advisories/ICSA-17-285-05

19. **SUSE**

https://www.suse.com/support/update/announcement/2017/suse-su-20172655-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172659-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172660-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172666-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172688-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172690-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172694-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172695-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172696-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172697-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172699-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172700-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172701-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172704-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172715-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172716-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172717-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172718-1/

20. **Symantec Products**

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20171009_00

21. **Ubuntu**

https://usn.ubuntu.com/usn/usn-3424-2/
https://usn.ubuntu.com/usn/usn-3440-1/
https://usn.ubuntu.com/usn/usn-3441-1/
https://usn.ubuntu.com/usn/usn-3442-1/
https://usn.ubuntu.com/usn/usn-3443-1/
https://usn.ubuntu.com/usn/usn-3443-2/
https://usn.ubuntu.com/usn/usn-3443-3/
https://usn.ubuntu.com/usn/usn-3444-1/
https://usn.ubuntu.com/usn/usn-3444-2/
https://usn.ubuntu.com/usn/usn-3445-1/
https://usn.ubuntu.com/usn/usn-3445-2/
https://usn.ubuntu.com/usn/usn-3446-1/
https://usn.ubuntu.com/usn/usn-3447-1/
https://usn.ubuntu.com/usn/usn-3448-1/
https://usn.ubuntu.com/usn/usn-3449-1/
https://usn.ubuntu.com/usn/usn-3450-1/
https://usn.ubuntu.com/usn/usn-3451-1/
https://usn.ubuntu.com/usn/usn-3452-1/
https://usn.ubuntu.com/usn/usn-3453-1/
https://usn.ubuntu.com/usn/usn-3454-1/

22. **WECON Technology Co., Ltd. LeviStudio HMI Editor**

https://ics-cert.us-cert.gov/advisories/ICSA-17-285-02

23. **Wireshark**

https://www.wireshark.org/security/wnpa-sec-2017-42.html
https://www.wireshark.org/security/wnpa-sec-2017-43.html
https://www.wireshark.org/security/wnpa-sec-2017-44.html

https://www.wireshark.org/security/wnpa-sec-2017-45.html
https://www.wireshark.org/security/wnpa-sec-2017-46.html

Sources of product vulnerability information:

Apple
CentOS
Debian
F5
Gentoo Linux
HKCERT
IBM
ICS-CERT
Juniper
Mageia
Microsoft
Oracle Linux
Red Hat
Slackware
SUSE
Symantec
Ubuntu
Wireshark

Contacts:

cert@govcert.gov.hk