GovCERT.HK

Weekly IT Security News Bulletin, 2020-W53

28 December 2020 – 3 January 2021

Headlines

"Swatting" with compromised home devices

- The law enforcement in the United States (US) recently received a number of reports of "swatting" incidents from manufacturers of smart home devices. Swatting is a kind of hoax where a prankster making deceptive calls to an authority for reporting fake emergency situation and requesting services to victim's location.
- Different from traditional swatting, the pranksters first hijack the victims' smart home devices with video and audio capabilities so that they can remotely watch the live stream footage and instantly respond to the emergency authorities or even share the live stream in online platforms.
- It was found that the victims might have re-used the same password for different accounts and this allowed the pranksters to gain access to victims' smart home devices by using the compromised passwords.
- There is an increasing trend of swatting observed across the US. Swatting can be a dangerous act and there was a case where an innocent person was accidentally shot dead by the police receiving a hoax call.

Advice

- Review the security of home devices with Internet access and ensure proper data encryption and user authentication are in place.
- Use strong password and adopt multi-factor authentication if available.
- Avoid using the same password for different user accounts or online services.
- Apply patches on all the home devices in a timely manner.
- Switch off home devices with video or audio capabilities when not in use.

Sources

- Threatpost
- ZDNet

Cross layer attacks through flawed random number generator

- A security researcher recently published a paper on how to exploit the weakness in pseudo-random number generator (PRNG) in Linux kernel to mount network attacks including DNS cache poisoning. Such attack is named as cross layer attack as it leverages vulnerabilities in multiple network protocol layers to attack the target systems with flawed PRNG.

- PRNG is used in the generation algorithms for IPv4 ID, IPv6 flow label and UDP source port. By inferring the internal state of PRNG from one OSI layer, an attacker can effectively predict the random number value in other layers. With knowledge of the internal states of PRNG, an attacker can predict the UDP source port which is one of the secrets to be obtained for launching DNS cache poisoning. While the attacker still has to perform guessing on the transaction ID, such approach can significantly reduce the time needed for a brute force attack from a couple of days to less than a minute.

- The researcher estimated that 3-5% web servers could possibly meet the pre-conditions for exploitation. The Linux security team was informed about the flaw and had developed a patch to fix it.

Advice

- Adopt Domain Name System Security Extensions (DNSSEC) to provide authentication on DNS data exchange.
- Set a short period for timeout for DNS queries to avoid brute-force of source port and injection of malicious responses.
- Adopt latest patches on operating systems and applications.

Sources

- arVix.org
- The Daily Swig

Product Vulnerability Notes & Security Updates

1. Debian

https://www.debian.org/security/2020/dsa-4818
https://www.debian.org/security/2020/dsa-4819
https://www.debian.org/security/2020/dsa-4820
https://www.debian.org/security/2020/dsa-4821

2. F5 Products

https://support.f5.com/csp/article/K00409335
https://support.f5.com/csp/article/K16124204
https://support.f5.com/csp/article/K83271321

3. Gentoo Linux

https://security.gentoo.org/glsa/202012-22
https://security.gentoo.org/glsa/202012-23
https://security.gentoo.org/glsa/202012-24

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201230-01-pe-en

5. McAfee Network Security Manager (NSM)

https://kc.mcafee.com/corporate/index?page=content&id=SB10341

6. QNAP Products

https://www.qnap.com/en/security-advisory/qsa-20-21
https://www.qnap.com/en/security-advisory/qsa-20-22
https://www.qnap.com/en/security-advisory/qsa-20-23

7. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20203933-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203934-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203938-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203939-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203940-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203944-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203945-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014590-1/

Sources of product vulnerability information:

- Debian
- F5
- Gentoo Linux
- Huawei
- McAfee
- QNAP
- SUSE

Contact:

cert@govcert.gov.hk