GovCERT.HK

Weekly IT Security News Bulletin, 2021-W14

5 April – 11 April 2021

Headlines

Security risks in third-party app stores

- While Google Play is the official hub for downloading Android apps, some users may turn to other app stores which can put them at risks. Security vendors recently found that APKPure, a popular third-party Android app store, was infected with Trojan dropper in its advertisement SDK for distributing Trojans. It could obtain and run a payload for performing various malicious actions like showing advertisement on lock screen, opening browser tabs, retrieving device information, and downloading other malware.

- The malware to be downloaded depends on the Android version of the devices. For example, devices with older Android version without security patches would be loaded with xHelper, which could grant hackers with root access on the devices. For devices with more current Android versions, they would be subject to risks of having paid subscriptions and intrusive advertisements. The developers of APKPure was informed and released an update version of APKPure to fix the issue on 9 April.

- Besides APKPure, malware was also found in AppGallery, an app store from a mobile device manufacturer, and over half of a million users had installed the infected apps. The malware, called Joker, when launched would establish connection to C2 servers for getting necessary configuration and retrieve additional components which could automatically subscribe and activate premium phone services by intercepting all SMS messages and transmitting them to the C2 server so as to allow malicious actors to gain commissions from the transactions. After being informed about the issue, AppGallery hid those malicious apps in the store and promised to conduct investigation.

Advice

- Always download apps from official or trusted sources.
- Apply security patches to apps and operating systems in a timely manner.
- Regularly perform full anti-malware scan on devices.

Sources

- Kaspersky
- Dark Reading
- Bleeping Computer
- Dr. Web
- The Record

Setting up defense against firmware attacks

- Firmware is a critical part of computing systems which may have privileged access to systems and sensitive information like credentials stored and processed in the memory. Any vulnerability in it can pose severe security risks. According to the National Vulnerability Database of National Institute of Standards and Technology, the number of firmware attacks has increased by five times in the last four years. This echoes with a recent survey conducted by Microsoft which showed that firmware attacks had become an emerging threat while many organisations were not well prepared for that.

- The survey indicated that over 80% of enterprises encountered one or more firmware attacks in the past two years, but only 29% of security budgets were allocated for firmware security and 21% confirmed that their firmware data was not monitored. For the measures adopted by organisations, about 46% and 36% organisations had invested in hardware-based kernel protection and memory encryption respectively. As priority was mostly accorded to incident detection and response, only 39% of security teams spent time on prevention of firmware attacks.

- Most organisations were lacking the resources for high-impact security work as their resources were usually given to lower-yield manual work like software patching and mitigation of vulnerabilities. In fact, security teams on average spent about 40% of time on firmware patches which could be automated. About 60% respondents thought that more effort should be invested in strategic work like strategy and preparation for sophisticated threats.

Advice

- Regular review the security of devices and updates the firmware to fix any known vulnerabilities in a timely manner.
- Review and choose those devices and operating systems with advanced security features such as kernel data protection and memory encryption to protect system kernel, memory, and drivers from attacks.

Sources

- Mircosoft
- Cyware

Product Vulnerability Notes & Security Updates

1. Android

https://source.android.com/security/bulletin/pixel/2021-04-01

2. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-tu79hvkO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-inf-disc-wCxZNjL2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-pqVYwyb
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-selfcare-VRWWWHgE
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-xss-U2WTsUg6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-inject-gbZGHP5T
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-andro-iac-f3UR8frB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-VObwRKWV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cmdinj-vsKGherc

3. Debian

https://www.debian.org/security/2021/dsa-4882
https://www.debian.org/security/2021/dsa-4883
https://www.debian.org/security/2021/dsa-4884
https://www.debian.org/security/2021/dsa-4885
https://www.debian.org/security/2021/dsa-4886

4. F5 BIG-IQ Centralized Management

https://support.f5.com/csp/article/K00843201

5. FATEK Automation WinProladder

https://us-cert.cisa.gov/ics/advisories/icsa-21-098-01

6. Fortinet Products

https://www.fortiguard.com/psirt/FG-IR-19-244
https://www.fortiguard.com/psirt/FG-IR-20-076
https://www.fortiguard.com/psirt/FG-IR-21-007

7. FreeBSD

https://www.freebsd.org/security/advisories/FreeBSD-SA-21:08.vm.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-21:09.accept_filter.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-21:10.jail_mount.asc

8. Hitachi ABB Power Grids Multiple Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-096-01

9. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-doublefree-en

10. IBM InfoSphere Information Server

https://www.ibm.com/support/pages/node/6438925

11. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-1068.html
https://linux.oracle.com/errata/ELSA-2021-1071.html
https://linux.oracle.com/errata/ELSA-2021-1072.html
https://linux.oracle.com/errata/ELSA-2021-1093.html
https://linux.oracle.com/errata/ELSA-2021-1135.html
https://linux.oracle.com/errata/ELSA-2021-1145.html
https://linux.oracle.com/errata/ELSA-2021-9121.html
https://linux.oracle.com/errata/ELSA-2021-9150.html
https://linux.oracle.com/errata/ELSA-2021-9151.html
https://linux.oracle.com/errata/ELSA-2021-9164.html

12. Red Hat

https://access.redhat.com/errata/RHSA-2021:1005
https://access.redhat.com/errata/RHSA-2021:1006
https://access.redhat.com/errata/RHSA-2021:1007
https://access.redhat.com/errata/RHSA-2021:1063
https://access.redhat.com/errata/RHSA-2021:1064
https://access.redhat.com/errata/RHSA-2021:1068
https://access.redhat.com/errata/RHSA-2021:1069
https://access.redhat.com/errata/RHSA-2021:1070
https://access.redhat.com/errata/RHSA-2021:1071
https://access.redhat.com/errata/RHSA-2021:1072
https://access.redhat.com/errata/RHSA-2021:1073
https://access.redhat.com/errata/RHSA-2021:1074
https://access.redhat.com/errata/RHSA-2021:1081
https://access.redhat.com/errata/RHSA-2021:1086
https://access.redhat.com/errata/RHSA-2021:1125
https://access.redhat.com/errata/RHSA-2021:1129
https://access.redhat.com/errata/RHSA-2021:1131
https://access.redhat.com/errata/RHSA-2021:1135
https://access.redhat.com/errata/RHSA-2021:1145

13. **Rockwell Automation FactoryTalk AssetCentre**

https://us-cert.cisa.gov/ics/advisories/icsa-21-091-01

14. **Slackware**

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.343456
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.424914

15. **SUSE**

https://www.suse.com/support/update/announcement/2021/suse-su-20211006-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211007-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211008-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211009-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211010-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211023-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211028-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211029-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211030-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211046-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211074-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211075-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211094-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211097-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211103-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211104-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211107-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211108-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211111-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211113-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114684-1/

16. **Symantec Products**

https://support.broadcom.com/security-advisory/content/security-advisories/OpenSSL-Vulnerabilities-Mar-2021/SYMSA17849

17. **Ubuntu**

https://ubuntu.com/security/notices/USN-4561-2
https://ubuntu.com/security/notices/USN-4896-2
https://ubuntu.com/security/notices/USN-4899-1
https://ubuntu.com/security/notices/USN-4900-1
https://ubuntu.com/security/notices/USN-4901-1
https://ubuntu.com/security/notices/USN-4902-1
https://ubuntu.com/security/notices/USN-4903-1

18. **VMware**

https://www.vmware.com/security/advisories/VMSA-2021-0005.html

Sources of product vulnerability information:

- Android
- Broadcom
- Cisco
- Debian
- F5
- Fortinet
- FreeBSD
- Huawei
- IBM
- Oracle Linux
- Red Hat
- Slackware
- SUSE
- Ubuntu
- US-CERT
- VMware

Contact:

cert@govcert.gov.hk