GovCERT.HK

Weekly IT Security News Bulletin, 2021-W10

8 March – 14 March 2021

Headlines

Threat Landscape in 2020

- According to a report summarising the global threat landscape in last year, ransomware was the most common threat type, accounting for about 23% of all attacks observed and followed by data threat (13%) and server access (10%). When launching ransomware attack, cybercriminals would first gain access to target systems through remote desktop protocol, credential theft and phishing. As many organisations have the practices to backup their data and would not consider to pay ransom for data recovery, cybercriminals now adopt a double extortion approach to not only encrypt but also exfiltrate the data and threaten to disclose it if victims do not pay the ransom. It was also found that the stolen data was sold in auctions held by ransomware providers on the dark web and such data leaks account for about 36% public breaches.

- Another finding is that 35% of attacks leveraged vulnerabilities. Among the top 10 most commonly exploited vulnerabilities, only two of the vulnerabilities were first discovered in 2020 and others were old vulnerabilities from 2019 or earlier. This shows that old vulnerabilities still have continuous and significant threats to cyber security. This phenomenon could possibly be explained by the difficulty in exploiting most of the vulnerabilities found in 2020 and the difficulty in some organisations in fixing those old vulnerabilities. This also contributed to the proliferation of scan and exploit attack (the most common attack vector in 2020) which requires less resources and can be automated.

Advice

- Regular backups should be done and sufficient backup copies should be kept to facilitate file recovery whenever necessary.
- Implement intrusion detection strategy at critical nodes of the network to detect abnormal activities.
- Stay vigilant of any vulnerabilities found in the applications and systems deployed in your environment and apply security patches to fix the vulnerabilities in a timely manner.

Sources

- IBM
- Security Intelligence

Software code signing through Sigstore

- Software supply chain is a natural target to exploit. With a view to strengthening the security of software supply chain, the Linux Foundation, together with Red Hat, Google, and Purdue University, has recently launched a free service called Sigstore for software developers to digitally sign their software artifacts such as release files, container images and binaries and store those signed materials in a tamper-proof public log.

- Software code signing is used by software developers as proof that their software code is originated from them without being tampered with by any third party. This assures the users that the software being used is from a trusted source.

- Different from the conventional code signing approach that requires a certificate from a certificate authority, Sigstore leverages OpenID authentication protocol to associate certificates with identities so that developers can use their own email account with an existing OpenID identity provider to sign their software. Sigstore can also help improve the transparency of software supply chain by maintaining a public log of signed materials. Developers can use the log to monitor any unknown changes in their software code so as to detect any account compromise or software being signed by malicious parties.

Advice

- Apply digital signing for public use software, such as mobile app, before release.
- Adopt application whitelisting approach to allow only trusted software to run in the IT environment.
- Verify the authenticity and integrity of the software before accepting the installation in the IT environment.

Sources

- Sigstore
- CSO Online
- Dark Reading

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/en-us/HT212220
https://support.apple.com/en-us/HT212223

2. F5 Products

https://support.f5.com/csp/article/K01243064
https://support.f5.com/csp/article/K02333782
https://support.f5.com/csp/article/K03009991
https://support.f5.com/csp/article/K06440657
https://support.f5.com/csp/article/K13155201
https://support.f5.com/csp/article/K16352404
https://support.f5.com/csp/article/K18132488
https://support.f5.com/csp/article/K27238230
https://support.f5.com/csp/article/K30585021
https://support.f5.com/csp/article/K31025212
https://support.f5.com/csp/article/K31934524
https://support.f5.com/csp/article/K32380005
https://support.f5.com/csp/article/K34074377
https://support.f5.com/csp/article/K34441555
https://support.f5.com/csp/article/K43470422
https://support.f5.com/csp/article/K44945790
https://support.f5.com/csp/article/K45056101
https://support.f5.com/csp/article/K52510511
https://support.f5.com/csp/article/K55237223
https://support.f5.com/csp/article/K56715231
https://support.f5.com/csp/article/K66851119
https://support.f5.com/csp/article/K67830124
https://support.f5.com/csp/article/K68251873
https://support.f5.com/csp/article/K70031188

3. Google Chrome

https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_5.html

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210310-01-escalation-en

5. IBM Db2

https://www.ibm.com/support/pages/node/6427855
https://www.ibm.com/support/pages/node/6427859
https://www.ibm.com/support/pages/node/6427861

6. McAfee Endpoint Product Removal (EPR) Tool

https://kc.mcafee.com/corporate/index?page=content&id=SB10351

7. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-0696.html
https://linux.oracle.com/errata/ELSA-2021-0705.html
https://linux.oracle.com/errata/ELSA-2021-0706.html
https://linux.oracle.com/errata/ELSA-2021-0711.html
https://linux.oracle.com/errata/ELSA-2021-0734.html
https://linux.oracle.com/errata/ELSA-2021-0735.html
https://linux.oracle.com/errata/ELSA-2021-0742.html
https://linux.oracle.com/errata/ELSA-2021-0788.html
https://linux.oracle.com/errata/ELSA-2021-0790.html
https://linux.oracle.com/errata/ELSA-2021-0793.html
https://linux.oracle.com/errata/ELSA-2021-0808.html
https://linux.oracle.com/errata/ELSA-2021-0809.html
https://linux.oracle.com/errata/ELSA-2021-9084.html
https://linux.oracle.com/errata/ELSA-2021-9085.html
https://linux.oracle.com/errata/ELSA-2021-9086.html
https://linux.oracle.com/errata/ELSA-2021-9100.html
https://linux.oracle.com/errata/ELSA-2021-9101.html
https://linux.oracle.com/errata/ELSA-2021-9104.html

8. Red Hat

https://access.redhat.com/errata/RHSA-2021:0713
https://access.redhat.com/errata/RHSA-2021:0738
https://access.redhat.com/errata/RHSA-2021:0739
https://access.redhat.com/errata/RHSA-2021:0740
https://access.redhat.com/errata/RHSA-2021:0741
https://access.redhat.com/errata/RHSA-2021:0742
https://access.redhat.com/errata/RHSA-2021:0743
https://access.redhat.com/errata/RHSA-2021:0744
https://access.redhat.com/errata/RHSA-2021:0758
https://access.redhat.com/errata/RHSA-2021:0759
https://access.redhat.com/errata/RHSA-2021:0760
https://access.redhat.com/errata/RHSA-2021:0761
https://access.redhat.com/errata/RHSA-2021:0763
https://access.redhat.com/errata/RHSA-2021:0765
https://access.redhat.com/errata/RHSA-2021:0771
https://access.redhat.com/errata/RHSA-2021:0774
https://access.redhat.com/errata/RHSA-2021:0778
https://access.redhat.com/errata/RHSA-2021:0779
https://access.redhat.com/errata/RHSA-2021:0787
https://access.redhat.com/errata/RHSA-2021:0788
https://access.redhat.com/errata/RHSA-2021:0789
https://access.redhat.com/errata/RHSA-2021:0790
https://access.redhat.com/errata/RHSA-2021:0793
https://access.redhat.com/errata/RHSA-2021:0794
https://access.redhat.com/errata/RHSA-2021:0808
https://access.redhat.com/errata/RHSA-2021:0809
https://access.redhat.com/errata/RHSA-2021:0811

9. Schneider Electric IGSS SCADA Software

https://us-cert.cisa.gov/ics/advisories/icsa-21-070-01

10. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-068-02
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-03
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-04
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-07
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-09
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-10

11. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210720-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210721-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210722-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210723-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210724-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210725-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210735-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210736-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210737-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210738-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210739-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210740-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210741-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210742-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210743-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210744-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210745-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210752-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210753-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210754-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210755-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210756-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210757-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210768-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210769-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210770-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210771-1/

12. Symantec Products

https://support.broadcom.com/security-advisory/content/security-advisories/OpenSSL-Vulnerabilities-Sep-2020-Feb-2021/SYMSA17570

13. Ubuntu

https://ubuntu.com/security/notices/USN-4733-2
https://ubuntu.com/security/notices/USN-4758-1
https://ubuntu.com/security/notices/USN-4759-1
https://ubuntu.com/security/notices/USN-4760-1
https://ubuntu.com/security/notices/USN-4761-1
https://ubuntu.com/security/notices/USN-4762-1
https://ubuntu.com/security/notices/USN-4763-1

14. Wireshark

https://www.wireshark.org/security/wnpa-sec-2021-03.html

15. Xen

https://xenbits.xen.org/xsa/advisory-367.html
https://xenbits.xen.org/xsa/advisory-369.html

Sources of product vulnerability information:

Apple
Broadcom
F5
Google Chrome
Huawei
IBM
McAfee
Oracle Linux
Red Hat
SUSE
Ubuntu
US-CERT
Wireshark
Xen

Contact:

cert@govcert.gov.hk