GovCERT.HK

Weekly IT Security News Bulletin, 2021-W07

15 February – 21 February 2021

Headlines

Unprecedentedly large number of vulnerabilities found in 2020

- A security vendor recently published a report highlighting some observations on the trends of security vulnerabilities from an analysis on the National Vulnerability Database (NVD) from the National Institute of Standards and Technology (NIST).

- It shows that a record high number of vulnerabilities (over 18,000) were discovered in 2020, where 57% of them were "critical" or "high severity" and 63% were of low complexity. The growth in number of vulnerabilities can be attributed to the proliferation of devices and products with network connectivity.

- It should also be noted that many vulnerabilities require no user interaction (68%) or user privileges (58%) to exploit. Attacks against such vulnerabilities can be difficult to detect and defend if no user action (e.g., clicking malicious links or opening malicious files) is needed. Without requiring any user privilege, it can save attackers much effort in finding a way like phishing to obtain the necessary privilege so as to compromise the target systems.

- While the percentage of critical and high severity vulnerabilities has decreased, attackers may still be able to first exploit the vulnerabilities of lower severity and perform chained attack to achieve the malicious goals.

Advice

- Stay alert for any vulnerabilities exist in your environment and get a full understanding of their risks and impact so as to identify and prioritise mitigation actions.
- Maintain an up-to-date inventory list of IT assets and have proper patch management to ensure vulnerabilities are patched in a timely manner.

Sources

- Redscan
- Cyware

Data Exfiltration using Google Apps scripts

- A security researcher recently discovered that malicious groups were exploiting Google Apps scripts to exfiltrate credit card information stolen from online stores.

- While the online stores may have Content Security Policy (CSP) configured to fend off code injection attacks by detecting and blocking execution of untrusted code or content, the domains associated with Google including Google Apps Script are usually whitelisted. In the concerned attack, a legitimate Google domain (script.google.com) was used by the hackers to hide their malicious activity from malware detection and circumvent the CSP controls.

- Malicious Javascripts were injected into the online stores for collecting payment and personal information of the customers. To exfiltrate those stolen data from the online stores, the data was encoded and sent to a Google Apps Script custom app, where the data was further relayed to the server controlled by hackers.

- In fact, the credit card skimmers have previously abused other Google services like Google Analytics and Google Forms to steal payment information on e-commerce websites.

Advice

- Configure and review the CSP based on business needs and associated security risks.
- Perform regular malware and vulnerability scanning to avoid malware infection or code injection.
- Set up monitoring on network traffic to detect any malicious activities including data exfiltration.

Sources

- Eric Brandel
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-hijac-JrcTOQMC
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-exp-8RsuEu8S
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-StarOS-DoS-RLLvGFJj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wda-pt-msh-6LWOcZ5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-Lz6HbGCt

2. Debian

https://www.debian.org/security/2021/dsa-4851
https://www.debian.org/security/2021/dsa-4852
https://www.debian.org/security/2021/dsa-4853
https://www.debian.org/security/2021/dsa-4854
https://www.debian.org/security/2021/dsa-4855
https://www.debian.org/security/2021/dsa-4856

3. F5 products

https://support.f5.com/csp/article/K24624116
https://support.f5.com/csp/article/K52833764
https://support.f5.com/csp/article/K61903372
https://support.f5.com/csp/article/K63525058

4. Google Chrome

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html

5. IBM WebSphere Application Server

https://www.ibm.com/support/pages/node/6415639
https://www.ibm.com/support/pages/node/6415959

6. Johnson Controls Metasys Reporting Engine (MRE) Web Services

https://us-cert.cisa.gov/ics/advisories/icsa-21-049-01

7. McAfee Products

https://kc.mcafee.com/corporate/index?page=content&id=SB10348
https://kc.mcafee.com/corporate/index?page=content&id=SB10349

8. Microsoft Edge (Chromium-based)

https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#february-17-2021

9. Mitsubishi Electric FA engineering software products

https://us-cert.cisa.gov/ics/advisories/icsa-21-049-02

10. Multiple Embedded TCP/IP stacks

https://us-cert.cisa.gov/ics/advisories/icsa-21-042-01

11. Open Design Alliance Drawings SDK

https://us-cert.cisa.gov/ics/advisories/icsa-21-047-01

12. OpenSSL

https://www.openssl.org/news/secadv/20210216.txt

13. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-0471.html
https://linux.oracle.com/errata/ELSA-2021-0474.html
https://linux.oracle.com/errata/ELSA-2021-0476.html
https://linux.oracle.com/errata/ELSA-2021-0538.html
https://linux.oracle.com/errata/ELSA-2021-0557.html
https://linux.oracle.com/errata/ELSA-2021-0558.html
https://linux.oracle.com/errata/ELSA-2021-9051.html
https://linux.oracle.com/errata/ELSA-2021-9052.html
https://linux.oracle.com/errata/ELSA-2021-9053.html
https://linux.oracle.com/errata/ELSA-2021-9057.html
https://linux.oracle.com/errata/ELSA-2021-9058.html

14. PHP

https://www.php.net/ChangeLog-7.php#7.3.27
https://www.php.net/ChangeLog-7.php#7.4.15

15. Red Hat

https://access.redhat.com/errata/RHSA-2021:0423
https://access.redhat.com/errata/RHSA-2021:0436
https://access.redhat.com/errata/RHSA-2021:0485
https://access.redhat.com/errata/RHSA-2021:0486
https://access.redhat.com/errata/RHSA-2021:0488
https://access.redhat.com/errata/RHSA-2021:0489
https://access.redhat.com/errata/RHSA-2021:0491
https://access.redhat.com/errata/RHSA-2021:0494
https://access.redhat.com/errata/RHSA-2021:0495
https://access.redhat.com/errata/RHSA-2021:0497
https://access.redhat.com/errata/RHSA-2021:0507
https://access.redhat.com/errata/RHSA-2021:0508
https://access.redhat.com/errata/RHSA-2021:0509
https://access.redhat.com/errata/RHSA-2021:0516
https://access.redhat.com/errata/RHSA-2021:0521
https://access.redhat.com/errata/RHSA-2021:0526
https://access.redhat.com/errata/RHSA-2021:0530
https://access.redhat.com/errata/RHSA-2021:0531
https://access.redhat.com/errata/RHSA-2021:0537

https://access.redhat.com/errata/RHSA-2021:0538
https://access.redhat.com/errata/RHSA-2021:0548
https://access.redhat.com/errata/RHSA-2021:0549
https://access.redhat.com/errata/RHSA-2021:0551
https://access.redhat.com/errata/RHSA-2021:0557
https://access.redhat.com/errata/RHSA-2021:0558
https://access.redhat.com/errata/RHSA-2021:0568
https://access.redhat.com/errata/RHSA-2021:0599
https://access.redhat.com/errata/RHSA-2021:0600
https://access.redhat.com/errata/RHSA-2021:0603
https://access.redhat.com/errata/RHSA-2021:0607
https://access.redhat.com/errata/RHSA-2021:0611

16. Rockwell Automation Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-042-02
https://us-cert.cisa.gov/ics/advisories/icsa-21-047-02

17. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210432-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210433-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210434-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210435-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210436-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210437-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210438-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210439-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210440-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210443-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210445-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210446-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210448-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210449-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210451-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210452-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210477-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210478-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210479-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210480-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210483-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210486-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210488-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210489-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210491-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210492-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210494-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210498-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210503-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210504-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210507-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210512-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210515-1/

https://www.suse.com/support/update/announcement/2021/suse-su-202114624-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114627-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114630-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114632-1/

18. Ubuntu

https://ubuntu.com/security/notices/USN-4732-1
https://ubuntu.com/security/notices/USN-4733-1
https://ubuntu.com/security/notices/USN-4734-1
https://ubuntu.com/security/notices/USN-4734-2
https://ubuntu.com/security/notices/USN-4735-1
https://ubuntu.com/security/notices/USN-4737-1
https://ubuntu.com/security/notices/USN-4738-1
https://ubuntu.com/security/notices/USN-4739-1
https://ubuntu.com/security/notices/USN-4740-1
https://ubuntu.com/security/notices/USN-4741-1

19. VMware

https://www.vmware.com/security/advisories/VMSA-2021-0001.html

20. Xen

https://xenbits.xen.org/xsa/advisory-361.html
https://xenbits.xen.org/xsa/advisory-362.html
https://xenbits.xen.org/xsa/advisory-363.html
https://xenbits.xen.org/xsa/advisory-364.html
https://xenbits.xen.org/xsa/advisory-365.html

Sources of product vulnerability information:

Cisco
Debian
F5
Google Chrome
IBM
McAfee
Microsoft
OpenSSL
Oracle Linux
PHP
Red Hat
SUSE
Ubuntu
US-CERT
VMware
Xen

Contact:

cert@govcert.gov.hk