GovCERT.HK

Weekly IT Security News Bulletin, 2021-W08

22 February – 28 February 2021

Headlines

Consolidation and collaboration as a key to secure networks

- A security researcher recently published an article highlighting the importance of effective consolidation and collaboration strategy in securing distributed corporate networks and systems.

- It is noted that many organisations, including large enterprises like IBM, deployed a number of security point solutions operating in isolation across their networks. Without a central security plan or strategy, security teams of such organisations have no way to launch a coordinated and consistent threat response with other solutions in the same segment of the network.

- To deal with new challenges in distributed clouds, extreme edge computing and smart environments, organisations are recommended to establish centralised security policy management, consistent enforcement, and proper configuration control. The best practice to achieve these objectives is to start with a two-pronged approach focused on consolidation and collaboration.

- Although other system enhancements such as performance tuning and AI integration are also valuable to organisations, the effectiveness of consolidation and collaboration strategy should still be considered as the top priority for organisations.

Advice

- Set up a common security framework using integrated security platform which supports multiple environment deployment, employs well-tested solutions, and owns a common operating system.
- Adopt SOAR (Security Orchestration, Automation and Response), SIEM (Security Information and Event Management), or XDR (eXtended Detection and Response) technologies to coordinate security systems and enhance interoperability between disparate solutions.

Sources

- SecurityWeek

Staying vigilant against AppleJeus malware

- The United States (U.S.) Government has identified a cryptocurrency malware, known as AppleJeus, which is used by threat actors to steal cryptocurrency from victims' cryptocurrency wallets. The U.S. Computer Emergency Readiness Team (US-CERT) has published reports detailing characteristics of AppleJeus and associated indicators of compromise (IoCs).

- AppleJeus, which was first discovered in 2018, is disguised as seemingly legitimate cryptocurrency trading applications to entice users to download the malware from seemingly legitimate cryptocurrency trading platforms and malicious links embedded in phishing emails. Once the malware is installed, attackers may gain access to the affected devices or organisations' networks for cryptocurrency theft.

- At present, there are seven versions of the AppleJeus malware, where all of them are capable of infecting both Windows and Mac operating system. Organisations from sectors including government and finance institutions are the major targets of the malware.

Advice

- Obtain software from official sources and perform anti-malware scanning on any software downloaded from the Internet.
- Avoid opening attachments or clicking links in unsolicited electronic messages, including but not limited to emails, instant messages, and SMS.
- Use dedicated device for processing cryptocurrency and adopt multi-factor authentication to protect user accounts.

Sources

- US-CERT
- SingCERT

Product Vulnerability Notes & Security Updates

1. Advantech Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-054-02
https://us-cert.cisa.gov/ics/advisories/icsa-21-054-03

2. Cisco AnyConnect

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dos-55AYyxYr

3. Debian

https://www.debian.org/security/2021/dsa-4857
https://www.debian.org/security/2021/dsa-4858
https://www.debian.org/security/2021/dsa-4859
https://www.debian.org/security/2021/dsa-4860
https://www.debian.org/security/2021/dsa-4861
https://www.debian.org/security/2021/dsa-4862
https://www.debian.org/security/2021/dsa-4863

4. F5 Products

https://support.f5.com/csp/article/K07944249
https://support.f5.com/csp/article/K15402727
https://support.f5.com/csp/article/K61186963

5. Fatek FvDesigner

https://us-cert.cisa.gov/ics/advisories/icsa-21-056-02

6. FreeBSD

https://www.freebsd.org/security/advisories/FreeBSD-SA-21:03.pam_login_access.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-21:04.jail_remove.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-21:05.jail_chdir.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-21:06.xen.asc

7. Google Chrome

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_22.html

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-0507.html
https://linux.oracle.com/errata/ELSA-2021-0531.html
https://linux.oracle.com/errata/ELSA-2021-0548.html
https://linux.oracle.com/errata/ELSA-2021-0549.html
https://linux.oracle.com/errata/ELSA-2021-0551.html
https://linux.oracle.com/errata/ELSA-2021-0611.html
https://linux.oracle.com/errata/ELSA-2021-0617.html
https://linux.oracle.com/errata/ELSA-2021-0618.html
https://linux.oracle.com/errata/ELSA-2021-0655.html
https://linux.oracle.com/errata/ELSA-2021-0656.html
https://linux.oracle.com/errata/ELSA-2021-9066.html
https://linux.oracle.com/errata/ELSA-2021-9067.html
https://linux.oracle.com/errata/ELSA-2021-9068.html

9. PerFact OpenVPN-Client

https://us-cert.cisa.gov/ics/advisories/icsa-21-056-01

10. ProSoft Technology ICX35

https://us-cert.cisa.gov/ics/advisories/icsa-21-056-04

11. Red Hat

https://access.redhat.com/errata/RHSA-2020:5364
https://access.redhat.com/errata/RHSA-2020:5633
https://access.redhat.com/errata/RHSA-2020:5634
https://access.redhat.com/errata/RHSA-2020:5635
https://access.redhat.com/errata/RHSA-2021:0100
https://access.redhat.com/errata/RHSA-2021:0617
https://access.redhat.com/errata/RHSA-2021:0618
https://access.redhat.com/errata/RHSA-2021:0619
https://access.redhat.com/errata/RHSA-2021:0620
https://access.redhat.com/errata/RHSA-2021:0648
https://access.redhat.com/errata/RHSA-2021:0650
https://access.redhat.com/errata/RHSA-2021:0651
https://access.redhat.com/errata/RHSA-2021:0655
https://access.redhat.com/errata/RHSA-2021:0656
https://access.redhat.com/errata/RHSA-2021:0659
https://access.redhat.com/errata/RHSA-2021:0663
https://access.redhat.com/errata/RHSA-2021:0664

12. Rockwell Automation Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-054-01
https://us-cert.cisa.gov/ics/advisories/icsa-21-056-03

13. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210521-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210522-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210527-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210528-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210529-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210530-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210531-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210532-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210533-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210536-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210543-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210544-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210545-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210549-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210551-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210563-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210565-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210583-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210584-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210594-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210597-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210599-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210600-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210601-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210602-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210603-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210605-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210607-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210608-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114634-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114640-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114644-1/

14. Ubuntu

https://ubuntu.com/security/notices/USN-4467-3
https://ubuntu.com/security/notices/USN-4698-2
https://ubuntu.com/security/notices/USN-4742-1
https://ubuntu.com/security/notices/USN-4743-1
https://ubuntu.com/security/notices/USN-4744-1
https://ubuntu.com/security/notices/USN-4745-1
https://ubuntu.com/security/notices/USN-4746-1
https://ubuntu.com/security/notices/USN-4747-1
https://ubuntu.com/security/notices/USN-4747-2
https://ubuntu.com/security/notices/USN-4748-1
https://ubuntu.com/security/notices/USN-4749-1
https://ubuntu.com/security/notices/USN-4750-1
https://ubuntu.com/security/notices/USN-4751-1
https://ubuntu.com/security/notices/USN-4752-1
https://ubuntu.com/security/notices/USN-4753-1
https://ubuntu.com/security/notices/USN-4754-1

https://ubuntu.com/security/notices/USN-4754-2
https://ubuntu.com/security/notices/USN-4755-1

15. Xen

https://xenbits.xen.org/xsa/advisory-366.html

Sources of product vulnerability information:

Cisco
Debian
F5
FreeBSD
Google Chrome
Oracle Linux
Red Hat
SUSE
Ubuntu
US-CERT
Xen

Contact:

cert@govcert.gov.hk