GovCERT.HK

Weekly IT Security News Bulletin, 2022-W09

28 February – 6 March 2022

Headlines

Malware signed with stolen certificates

- One of the world's leading chips and graphics processing units (GPU) manufacturers suffered a data breach of over 70,000 employee email addresses, password hashes, and proprietary information. The stolen information also included two valid code signing certificates currently being abused in malware campaigns.

- A code signing certificate is used by software developers to digitally sign their applications and software programs and allows users to verify the authenticity and integrity of the content. By default, the Windows system does not allow the installation of a driver not digitally signed with a trusted certificate. With the stolen certificates, threat actors could make malware appearing to be a valid GPU driver from the affected manufacturer.

- While one of the certificates was expired in 2014, malicious code signed with expired certificates can still be loaded by Windows systems. Fortunately, some anti-malware solution providers have updated their malware signatures to detect and block code signed by the rogue certificates.

Advice

- Enable anti-malware solution with latest malware signatures updated.
- Review security policies to ensure code recently signed by the rogue certificate is detected and blocked.
- Apply application whitelisting to ensure that only trusted code can be run.

Sources

- Bleeping Computer
- The Register

Misconfigured network middleboxes used in DDoS attacks

- Security researchers observed a new series of distributed denial of service (DDoS) attack technique known as TCP middlebox reflection attack. The technique allows attackers to abuse misconfigured network middleboxes such as firewalls and content filtering devices to amplify TCP attack traffic by over 65 times.

- This newly discovered attack technique involves sending specially crafted TCP packet sequences that contain spoofed source IP addresses of the intended victims and anomalous HTTP request headers with blacklisted domain names. Once received, the middleboxes would respond to the victims' IP addresses with HTTP headers or entire HTML pages, creating an amplification opportunity to attackers.

- Researchers found some network middleboxes not conforming to the TCP standard, resulting in responding to spoofed requests even if there is no valid TCP connection or handshake. In contrast with using Botnet to launch DDoS attacks, attackers can take advantage of TCP-noncompliance in the middleboxes to launch TCP reflection/amplification attacks without compromising the devices.

Advice

- Enable SYN challenges in firewalls to detect and drop malicious data flows.
- Use signature tools to drop cleartext patterns in the response traffic.
- Configure firewall rules to block the known incorrect patterns.

Sources

- Akamai
- Security Week
- The Hacker News

Product Vulnerability Notes & Security Updates

1. Becton, Dickinson and Company Products

https://us-cert.cisa.gov/ics/advisories/icsma-22-062-01
https://us-cert.cisa.gov/ics/advisories/icsma-22-062-02

2. CentOS

https://lists.centos.org/pipermail/centos-announce/2022-February/073559.html
https://lists.centos.org/pipermail/centos-announce/2022-February/073565.html
https://lists.centos.org/pipermail/centos-announce/2022-February/073566.html
https://lists.centos.org/pipermail/centos-announce/2022-February/073572.html
https://lists.centos.org/pipermail/centos-announce/2022-February/073573.html
https://lists.centos.org/pipermail/centos-announce/2022-March/073574.html

3. Debian

https://www.debian.org/security/2022/dsa-5087

4. F5 Products

https://support.f5.com/csp/article/K34519550
https://support.f5.com/csp/article/K42406850
https://support.f5.com/csp/article/K73200428

5. Fortinet

https://www.fortiguard.com/psirt/FG-IR-20-091
https://www.fortiguard.com/psirt/FG-IR-21-008
https://www.fortiguard.com/psirt/FG-IR-21-028
https://www.fortiguard.com/psirt/FG-IR-21-099
https://www.fortiguard.com/psirt/FG-IR-21-106
https://www.fortiguard.com/psirt/FG-IR-21-128
https://www.fortiguard.com/psirt/FG-IR-21-165
https://www.fortiguard.com/psirt/FG-IR-21-189
https://www.fortiguard.com/psirt/FG-IR-21-210
https://www.fortiguard.com/psirt/FG-IR-21-227
https://www.fortiguard.com/psirt/FG-IR-21-255

6. IPCOMM ipDIO

https://us-cert.cisa.gov/ics/advisories/icsa-22-062-01

7. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4UGIOR5OPYQTAQRTVNXBBH25LGJ74XJJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/5SJPZ2MSI7IPFCS5TFZZVXF4NN6XKYKJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6B3VSER4WPCPULJGLJVI75SE2NKX4RQH/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6TWLTKRSHNPCLQL7UXQSITHNYJT5XSK5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/7PDLGPMBD55VDGY5SOH7FHBZ3M4MY6JV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/47DECU4TVYMA4WKQLEFTNQZSSOK2IUZP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FPABDE53LLJDPCFTIOU2DXOPZRS7JPVT/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/G2JZKFAH5MWINMQLTSYZ2GQCLX5UGIGE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/H2Z7YY7HZ2IKSH75SHSRUFT5AJHJJOLN/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HDRFZQH6Q6RDEHYEK4JINRVGLORNWT6O/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/M7W5B54ZNEJAVL7GGOKD46WWECPPJUNF/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/NCH4EEBMT6XZIRNVGTNBOCQCY4JVZ4IN/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/O33XW3SB7IZV5RQWCSZCBFQE4OBWACOB/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SKV5JFO4OEUPAEZYKX2BZO27HN3SN3P5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/W7QEMHXA4R2RUIQPQL2RSCQ7TBADKDOH/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WUFXLLYPEPLGLE3CNOENBUDET76YJXPI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/YYNT2UJMLIROP7MHRZ44QD3U3AE6FYLK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ZQOIWU7XODRDIITDKWB45QLM5US3ATJW/

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-0323.html
https://linux.oracle.com/errata/ELSA-2022-0328.html
https://linux.oracle.com/errata/ELSA-2022-0332.html
https://linux.oracle.com/errata/ELSA-2022-0350.html
https://linux.oracle.com/errata/ELSA-2022-0366.html
https://linux.oracle.com/errata/ELSA-2022-0368.html
https://linux.oracle.com/errata/ELSA-2022-0370.html
https://linux.oracle.com/errata/ELSA-2022-0418.html
https://linux.oracle.com/errata/ELSA-2022-0672.html
https://linux.oracle.com/errata/ELSA-2022-9073.html
https://linux.oracle.com/errata/ELSA-2022-9088.html
https://linux.oracle.com/errata/ELSA-2022-9117.html

https://linux.oracle.com/errata/ELSA-2022-9177.html
https://linux.oracle.com/errata/ELSA-2022-9179.html
https://linux.oracle.com/errata/ELSA-2022-9180.html
https://linux.oracle.com/errata/ELSA-2022-9181.html
https://linux.oracle.com/errata/ELSA-2022-9182.html

9. Red Hat

https://access.redhat.com/errata/RHSA-2022:0655
https://access.redhat.com/errata/RHSA-2022:0682
https://access.redhat.com/errata/RHSA-2022:0687
https://access.redhat.com/errata/RHSA-2022:0708
https://access.redhat.com/errata/RHSA-2022:0718
https://access.redhat.com/errata/RHSA-2022:0721
https://access.redhat.com/errata/RHSA-2022:0722
https://access.redhat.com/errata/RHSA-2022:0727
https://access.redhat.com/errata/RHSA-2022:0728
https://access.redhat.com/errata/RHSA-2022:0730
https://access.redhat.com/errata/RHSA-2022:0731
https://access.redhat.com/errata/RHSA-2022:0735

10. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.343430
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.476921
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.486109

11. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220574-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220575-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220576-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220577-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220593-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220615-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220619-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220647-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220653-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220654-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220657-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220660-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220667-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220668-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220675-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220676-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220677-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220678-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220679-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220690-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220693-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20220694-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220695-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220696-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220698-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220699-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220702-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220703-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220704-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214898-1/

12. Ubuntu

https://ubuntu.com/security/notices/USN-5300-2
https://ubuntu.com/security/notices/USN-5303-1
https://ubuntu.com/security/notices/USN-5304-1
https://ubuntu.com/security/notices/USN-5305-1
https://ubuntu.com/security/notices/USN-5306-1
https://ubuntu.com/security/notices/USN-5307-1
https://ubuntu.com/security/notices/USN-5309-1
https://ubuntu.com/security/notices/USN-5310-1
https://ubuntu.com/security/notices/USN-5311-1
https://ubuntu.com/security/notices/USN-5312-1

13. VMware

https://www.vmware.com/security/advisories/VMSA-2022-0007.html

Sources of product vulnerability information:

CentOS
Debian
F5 Products
Fortinet
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
US-CERT
VMware

Contact:

cert@govcert.gov.hk