GovCERT.HK

Weekly IT Security News Bulletin, 2022-W05

31 January – 6 February 2022

Headlines

A shift toward behaviour-based detection

- Researchers have observed that threat actors are taking advantage of unusual programming languages for malware development. Malware written in unusual programming languages, such as DLang, Nim, Rust and Go, can easily evade signature-based detection, posing a security threat to organisations.

- Signature-based malware detection involves using a predefined repository of static signatures that represent known malware threats, e.g. a hash of malicious file. A known malware rewritten in other languages can create new static signatures, thereby undetected by anti-malware solutions using previously identified signatures of the original malware.

- Given that most malware spotted in the wild is not written in DLang, Nim, Rust and Go, malware analysts may not be familiar with the implementation of these unusual languages, making the task of identifying signatures more tedious. Researchers believed that it could be easier for threat actors to rewrite their original malware codes in uncommon languages, rather than changing their tactics, techniques, and procedures (TTP) to bypass malware detection.

Advice

- Deploy endpoint detection and response (EDR) with capability of behavioural analysis for effective detection of malicious code running across systems and networks.
- Monitor network traffic system and application logs to identify abnormal activities.

Sources

- Security Boulevard
- IronNet

Security flaws in UEFI firmware potentially impact millions of devices

- Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a device's firmware to the operating system for handling the booting process, system diagnostics, and repair functions. Researchers discovered 23 critical vulnerabilities in InsydeH2O's UEFI firmware code used by multiple major hardware vendors including Fujitsu, Siemens, Dell, HP, and Lenovo.

- The majority of the vulnerabilities were related to System Management Mode (SMM) which can lead to arbitrary code execution with SMM privileges on an affected device. SMM is a special-purpose operating mode on x86 and x86-64 processors used to perform low-level system management operations, such as power management and system hardware control. Attackers with SMM privileges could implant malicious code that survives from operating system reboot and re-installations.

- With the capability of bypassing security detection and maintaining persistence on the target device, the vulnerabilities could be used at the second stage in multi-stage malware attacks. MoonBounce was one of the malware that targeted UEFI firmware and interfered with Windows Kernel to deploy further malware.

Advice

- Regularly review and install the latest firmware from the trusted source.
- Conduct regular scans to detect known vulnerabilities.

Sources

- Binarly
- Security Affairs

Product Vulnerability Notes & Security Updates

1. **Advantech ADAM-3600**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-032-02

2. **Airspan Networks Mimosa**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-034-02

3. **CentOS**

   https://lists.centos.org/pipermail/centos-announce/2022-February/073554.html

4. **Debian**

   https://www.debian.org/security/2022/dsa-5064
   https://www.debian.org/security/2022/dsa-5065

5. **F5 Products**

   https://support.f5.com/csp/article/K05295469
   https://support.f5.com/csp/article/K28622040
   https://support.f5.com/csp/article/K34002344
   https://support.f5.com/csp/article/K40508224
   https://support.f5.com/csp/article/K46015513
   https://support.f5.com/csp/article/K54450124
   https://support.f5.com/csp/article/K67416037
   https://support.f5.com/csp/article/K74013101
   https://support.f5.com/csp/article/K84695749

6. **Fortinet**

   https://www.fortiguard.com/psirt/FG-IR-20-217
   https://www.fortiguard.com/psirt/FG-IR-21-132
   https://www.fortiguard.com/psirt/FG-IR-21-148
   https://www.fortiguard.com/psirt/FG-IR-21-158
   https://www.fortiguard.com/psirt/FG-IR-21-166
   https://www.fortiguard.com/psirt/FG-IR-21-180
   https://www.fortiguard.com/psirt/FG-IR-21-185

7. **Gentoo Linux**

   https://security.gentoo.org/glsa/202201-02
   https://security.gentoo.org/glsa/202202-01

8. **OpenSSL**

   https://www.openssl.org/news/secadv/20220128.txt

9. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6P5G6MJW4Q5RKKPO7TS5CLAAEQ2QUYBE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/72ZRNFZ3DE3TJA7HFCVV476YJN6I4B5M/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/543MEJC5CUZO2UZUL4R43HGV5KUNNJ4U/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/BCAASO7BUECWSWSJG3BJNIXSTKXZ4UYT/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/K7LELM65YZ36YQVKZDECL77ZYNXAWR6D/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/RB554CLNYEUAEMABV3LV3T5P4BYDLS7H/

10. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-0001.html
https://linux.oracle.com/errata/ELSA-2022-0003.html
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-2022-9073.html
https://linux.oracle.com/errata/ELSA-2022-9088.html
https://linux.oracle.com/errata/ELSA-2022-9117.html

11. Red Hat

https://access.redhat.com/errata/RHSA-2022:0283
https://access.redhat.com/errata/RHSA-2022:0323
https://access.redhat.com/errata/RHSA-2022:0325
https://access.redhat.com/errata/RHSA-2022:0328
https://access.redhat.com/errata/RHSA-2022:0329
https://access.redhat.com/errata/RHSA-2022:0330
https://access.redhat.com/errata/RHSA-2022:0331
https://access.redhat.com/errata/RHSA-2022:0332
https://access.redhat.com/errata/RHSA-2022:0335
https://access.redhat.com/errata/RHSA-2022:0344
https://access.redhat.com/errata/RHSA-2022:0345
https://access.redhat.com/errata/RHSA-2022:0366
https://access.redhat.com/errata/RHSA-2022:0368
https://access.redhat.com/errata/RHSA-2022:0370
https://access.redhat.com/errata/RHSA-2022:0397
https://access.redhat.com/errata/RHSA-2022:0400
https://access.redhat.com/errata/RHSA-2022:0401
https://access.redhat.com/errata/RHSA-2022:0404
https://access.redhat.com/errata/RHSA-2022:0405
https://access.redhat.com/errata/RHSA-2022:0406

https://access.redhat.com/errata/RHSA-2022:0407
https://access.redhat.com/errata/RHSA-2022:0408
https://access.redhat.com/errata/RHSA-2022:0409
https://access.redhat.com/errata/RHSA-2022:0410
https://access.redhat.com/errata/RHSA-2022:0415
https://access.redhat.com/errata/RHSA-2022:0418
https://access.redhat.com/errata/RHSA-2022:0420
https://access.redhat.com/errata/RHSA-2022:0421
https://access.redhat.com/errata/RHSA-2022:0422
https://access.redhat.com/errata/RHSA-2022:0430
https://access.redhat.com/errata/RHSA-2022:0431
https://access.redhat.com/errata/RHSA-2022:0432
https://access.redhat.com/errata/RHSA-2022:0434
https://access.redhat.com/errata/RHSA-2022:0435
https://access.redhat.com/errata/RHSA-2022:0436
https://access.redhat.com/errata/RHSA-2022:0437
https://access.redhat.com/errata/RHSA-2022:0438
https://access.redhat.com/errata/RHSA-2022:0439

12. Ricon Mobile Industrial Cellular Router

https://us-cert.cisa.gov/ics/advisories/icsa-22-032-01

13. Sensormatic PowerManage

https://us-cert.cisa.gov/ics/advisories/icsa-22-034-01

14. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.852695

15. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220225-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220226-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220241-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220251-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220252-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220254-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220255-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220257-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220262-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220263-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220267-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220270-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220271-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220277-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220283-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220284-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220285-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220286-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220287-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20220288-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220289-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220291-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220292-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220293-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220295-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220296-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220298-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220301-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220310-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220311-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220323-1/

16. Trend Micro

https://success.trendmicro.com/solution/000290434

17. Ubuntu

https://ubuntu.com/security/notices/USN-5030-2
https://ubuntu.com/security/notices/USN-5257-1
https://ubuntu.com/security/notices/USN-5259-1
https://ubuntu.com/security/notices/USN-5260-1
https://ubuntu.com/security/notices/USN-5260-2
https://ubuntu.com/security/notices/USN-5260-3
https://ubuntu.com/security/notices/USN-5262-1
https://ubuntu.com/security/notices/USN-5264-1
https://ubuntu.com/security/notices/USN-5265-1
https://ubuntu.com/security/notices/USN-5266-1
https://ubuntu.com/security/notices/USN-5267-1
https://ubuntu.com/security/notices/USN-5268-1
https://ubuntu.com/security/notices/USN-5269-1
https://ubuntu.com/security/notices/USN-5270-1
https://ubuntu.com/security/notices/USN-5270-2

18. VMware

https://www.vmware.com/security/advisories/VMSA-2022-0003.html

Sources of product vulnerability information:

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

Contact:

cert@govcert.gov.hk