GovCERT.HK

Weekly IT Security News Bulletin, 2022-W11

14 March – 20 March 2022

Headlines

New Linux botnet using DNS tunnelling for communication

- A previously undocumented botnet malware has been observed targeting Linux systems with ARM and x64 CPU architectures. The malware could allow attackers to steal sensitive information from a compromised device, download and install rootkits from a remote server, gain remote access to the device, and use the device to act as web traffic proxies.

- The malware, named B1txor20, debuted in February 2022 and was spread by exploiting the Log4J vulnerability in unpatched Linux systems. To conceal its malicious traffic, B1txor20 used DNS tunnelling to establish a communication channel with command and control (C2) servers by encoding data in DNS queries and responses.

- Once the device was compromised, the B1txor20 malware utilised the DNS tunnel to exfiltrate sensitive information, command execution results, and other information to C2 servers as a DNS request. Then, the device waited to execute any malicious commands sent by the C2 servers.

Advice

- Ensure that the latest security patches are applied to systems in a timely manner.
- Closely monitor DNS traffic to detect suspicious domains and unusual DNS queries to mitigate the risks of DNS tunnelling.

Sources

- Netlab 360
- BleepingComputer

New malware targeting Microsoft SQL and MySQL database servers

- Security researchers from AhnLab discovered a new variant of the Gh0stCringe remote access trojan targeting insecure Microsoft SQL and MySQL database servers. The Gh0stCringe malware was designed to perform various instructions based on custom commands received from command and control (C2) servers.

- Besides deploying additional malicious payloads from C2 servers, the Gh0stCringe malware comes with several functionalities ranging from keylogging to deleting the Master Boot Record (MBR) on the victim's machine to render the system unusable.

- According to AhnLab, the Gh0stCringe malware was known to be distributed through poorly managed database servers with weak account credentials that were subject to brute-force and dictionary attacks. In some cases, unpatched vulnerabilities were exploited to spread the Gh0stCringe malware.

Advice

- Apply the latest security updates to defend against any exploitation of known and unpatched vulnerabilities.
- Use strong and complex passwords for all systems and enable multi-factor authentication if applicable.
- Deploy security solutions such as firewall for all database servers to detect and block unauthorised access.

Sources

- AhnLab
- BleepingComputer

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/en-us/HT213183
https://support.apple.com/en-us/HT213184
https://support.apple.com/en-us/HT213185
https://support.apple.com/en-us/HT213187
https://support.apple.com/en-us/HT213188
https://support.apple.com/en-us/HT213189
https://support.apple.com/en-us/HT213190
https://support.apple.com/en-us/HT213191

2. ASEA Brown Boveri OPC Server for AC 800M

https://us-cert.cisa.gov/ics/advisories/icsa-22-074-01

3. Debian

https://www.debian.org/security/2022/dsa-5098
https://www.debian.org/security/2022/dsa-5099
https://www.debian.org/security/2022/dsa-5100
https://www.debian.org/security/2022/dsa-5101
https://www.debian.org/security/2022/dsa-5102
https://www.debian.org/security/2022/dsa-5103

4. F5 Products

https://support.f5.com/csp/article/K40778012
https://support.f5.com/csp/article/K63603485

5. FreeBSD

https://www.freebsd.org/security/advisories/FreeBSD-SA-22:02.wifi.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-22:03.openssl.asc

6. OpenSSL

https://www.openssl.org/news/secadv/20220315.txt

7. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4IS5FMKDHHRO4IBOMDW2TOCFQJ7BOXCY/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6422VZTPHB75VR6MKMLREZ5FDX6SVNHY/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/BZZMZMEXJXNF2NQNIXETAFBVRAZVIVSO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/D7KK2SNPNAB353QA6BU4SNJDQ3FXZOY5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/K2HM7MZLDNJ2W6HOMDMSHAZDFGLK43HO/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/KJ4E4JWVNOUJ5BNESH2IF34TBNSWMRGO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SF6GP7Y7QBDPSDEMYQPWKSOXKRHILQVP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/U4SBF2QAXCDZCB26LZTI2RH7Q33DJRIB/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/U6OQKLWM3DMDDCKHLY4KFE6NXSK5MSXV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/VXEFRXJEYR7QPAMYNWTJIYKTVX5OEQ7O/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WAE6CSZY5X5K62OKNSD5W35BIQQRELP4/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WYCKEL27LS2QTHCEAYFVLKKSZP4MBBJQ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/XL4H6UZUJ7J37CDBIJWGDOHX5XDWRWL6/

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-0826.html
https://linux.oracle.com/errata/ELSA-2022-0827.html
https://linux.oracle.com/errata/ELSA-2022-0830.html
https://linux.oracle.com/errata/ELSA-2022-0886.html
https://linux.oracle.com/errata/ELSA-2022-0889.html
https://linux.oracle.com/errata/ELSA-2022-0891.html
https://linux.oracle.com/errata/ELSA-2022-0892.html
https://linux.oracle.com/errata/ELSA-2022-0894.html
https://linux.oracle.com/errata/ELSA-2022-0896.html
https://linux.oracle.com/errata/ELSA-2022-0899.html
https://linux.oracle.com/errata/ELSA-2022-0951.html
https://linux.oracle.com/errata/ELSA-2022-9221.html
https://linux.oracle.com/errata/ELSA-2022-9227.html
https://linux.oracle.com/errata/ELSA-2022-9228.html
https://linux.oracle.com/errata/ELSA-2022-9229.html
https://linux.oracle.com/errata/ELSA-2022-9232.html

9. Red Hat

https://access.redhat.com/errata/RHSA-2022:0055
https://access.redhat.com/errata/RHSA-2022:0056
https://access.redhat.com/errata/RHSA-2022:0712
https://access.redhat.com/errata/RHSA-2022:0810
https://access.redhat.com/errata/RHSA-2022:0826
https://access.redhat.com/errata/RHSA-2022:0827
https://access.redhat.com/errata/RHSA-2022:0828
https://access.redhat.com/errata/RHSA-2022:0841
https://access.redhat.com/errata/RHSA-2022:0842
https://access.redhat.com/errata/RHSA-2022:0849
https://access.redhat.com/errata/RHSA-2022:0851
https://access.redhat.com/errata/RHSA-2022:0855
https://access.redhat.com/errata/RHSA-2022:0856
https://access.redhat.com/errata/RHSA-2022:0886
https://access.redhat.com/errata/RHSA-2022:0889

https://access.redhat.com/errata/RHSA-2022:0891
https://access.redhat.com/errata/RHSA-2022:0896
https://access.redhat.com/errata/RHSA-2022:0925
https://access.redhat.com/errata/RHSA-2022:0947
https://access.redhat.com/errata/RHSA-2022:0949
https://access.redhat.com/errata/RHSA-2022:0951
https://access.redhat.com/errata/RHSA-2022:0952
https://access.redhat.com/errata/RHSA-2022:0958

10. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.345883
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.474329
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.497803
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.523032

11. SonicWall Products

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001

12. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220810-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220811-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220814-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220815-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220816-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220817-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220818-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220819-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220820-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220821-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220822-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220825-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220826-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220828-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220832-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220841-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220842-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220843-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220844-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220845-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220847-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220851-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220853-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220854-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220856-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220857-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220859-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20220860-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220871-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220872-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220873-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220881-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220882-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220886-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220895-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214906-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214908-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214909-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214910-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214914-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214915-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214916-1/

13. Ubuntu

https://ubuntu.com/security/notices/USN-5321-2
https://ubuntu.com/security/notices/USN-5323-1
https://ubuntu.com/security/notices/USN-5324-1
https://ubuntu.com/security/notices/USN-5325-1
https://ubuntu.com/security/notices/USN-5327-1
https://ubuntu.com/security/notices/USN-5328-1
https://ubuntu.com/security/notices/USN-5328-2
https://ubuntu.com/security/notices/USN-5329-1
https://ubuntu.com/security/notices/USN-5330-1
https://ubuntu.com/security/notices/USN-5331-1
https://ubuntu.com/security/notices/USN-5332-1
https://ubuntu.com/security/notices/USN-5332-2
https://ubuntu.com/security/notices/USN-5333-1
https://ubuntu.com/security/notices/USN-5333-2
https://ubuntu.com/security/notices/USN-5334-1

Sources of product vulnerability information:

Apple
Debian
F5 Products
FreeBSD
OpenSSL
openSUSE
Oracle Linux
Red Hat
Slackware
SonicWall
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk