GovCERT.HK

Weekly IT Security News Bulletin, 2022-W14

4 April – 10 April 2022

Headlines

Phishing attacks masquerade as WhatsApp voice message

- Researchers have observed a new phishing campaign impersonating WhatsApp's voice message to spread information-stealing malware. The phishing campaign has reached at least 27,000 email addresses. The information stolen by the malware was predominately account credentials stored in browsers and applications but nevertheless, cryptocurrency wallets and SSH keys were also targeted.

- The phishing email with subject line "New Incoming Voice message" spoofed a voice notification message from WhatsApp and invited victims to click the "Play" button to listen to voice message. The sender appearing to be come from a "Whatsapp Notifier" service used an email address with a valid domain so as to evade email security solutions.

- If the recipient clicks on the "Play" button, a website would be opened and the browser would then show a popup notification to prompt victims to confirm "they are not a robot". After the confirmation, the information-stealing malware will be deployed as a Windows application through a browser Ad service and bypass Windows' User Account Control.

Advice

- Stay vigilant against unsolicited emails and messages even if they look official and legitimate as well as avoid opening any suspicious or unexpected links or attachments.
- Use robust endpoint security solutions and scan emails and web content for malicious payloads.
- Enable multi-factor authentication (MFA) for online accounts to minimise the risks of credential theft.

Sources

- Armorblox
- Bleeping Computer

The importance of prioritising API security

- The rapid growth in digital transformation drove Application Programming Interface (API) to play a key role in web and mobile application development with organisations relying on APIs to expand online services. While the APIs offer a series of benefits for organisations to provide both functionalities and agilities, the security aspect of API also emerges as a top priority in protecting sensitive data as cybercriminals are now targeting API more aggressively than ever before.

- Security researchers from Gartner predicted that API abuse would become the most common attack vector for enterprise web applications in 2022. According to a recent survey, 95% of organisations which implemented APIs in their systems have experienced incidents related to breaches in security and cyber attacks.

- Concerning the common security problems faced by production APIs, a research showed that 39% of the organisations identified security vulnerabilities as the major issue, followed by authentication issues (32%) and sensitive data exposure (30%). In addition, older versions of APIs were also more likely to be exploited as they are often deprecated without further patching or maintenance.

Advice

- Establish solid API security strategies and employ proper security solutions to protect their APIs from abusive calls
- Maintain clear API documentation and perform regular security scanning to check for potential security vulnerabilities in APIs.
- Deploy a web application firewall to protect API endpoints against web attacks.

Sources

- The Hacker News
- Salt Labs

Product Vulnerability Notes & Security Updates

1. ABB SPIET800 and PNI800

https://us-cert.cisa.gov/ics/advisories/icsa-22-097-02

2. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-spring-rce-Zx9GUc67
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-spring-scf-rce-DQrHhJxH

3. Citrix

https://support.citrix.com/article/CTX390511

4. Debian

https://www.debian.org/security/2022/dsa-5111
https://www.debian.org/security/2022/dsa-5112
https://www.debian.org/security/2022/dsa-5113

5. F5 Products

https://support.f5.com/csp/article/K08827426
https://support.f5.com/csp/article/K10002140
https://support.f5.com/csp/article/K29855410
https://support.f5.com/csp/article/K49419538
https://support.f5.com/csp/article/K51048910

6. Fortinet

https://www.fortiguard.com/psirt/FG-IR-21-002
https://www.fortiguard.com/psirt/FG-IR-21-060
https://www.fortiguard.com/psirt/FG-IR-21-062
https://www.fortiguard.com/psirt/FG-IR-21-064
https://www.fortiguard.com/psirt/FG-IR-21-065
https://www.fortiguard.com/psirt/FG-IR-21-070
https://www.fortiguard.com/psirt/FG-IR-21-078
https://www.fortiguard.com/psirt/FG-IR-21-226
https://www.fortiguard.com/psirt/FG-IR-21-232
https://www.fortiguard.com/psirt/FG-IR-21-238
https://www.fortiguard.com/psirt/FG-IR-22-018
https://www.fortiguard.com/psirt/FG-IR-22-019
https://www.fortiguard.com/psirt/FG-IR-22-052
https://www.fortiguard.com/psirt/FG-IR-22-059
https://www.fortiguard.com/psirt/FG-IR-22-072

7. **FreeBSD**

https://www.freebsd.org/security/advisories/FreeBSD-SA-22:04.netmap.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-22:05.bhyve.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-22:06.ioctl.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-22:07.wifi_meshid.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-22:08.zlib.asc

8. **Huawei Products**

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220406-01-bdb62b17-en

9. **IBM Products**

https://www.ibm.com/support/pages/node/6569505

10. **Johnson Controls Metasys**

https://us-cert.cisa.gov/ics/advisories/icsa-22-095-02

11. **LifePoint Informatics Patient Portal**

https://us-cert.cisa.gov/ics/advisories/icsma-22-095-01

12. **openSUSE**

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4ITLKQDHCBVY73BXRDDHU7JJZJG7TVNG/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/42XLX5GUN36HINIJX75C5RSFWMGRN4OW/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/76BLKP3BHKRBWFX4VJKKQJQXQTYEOOSX/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FCF4T6UJ7XULLDWSL3BELHJR3LWCF4TI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/U5JRSH3JEFDRI2LLKIUVXRRMZJAO5ZPH/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ULIK4RFHGHTVVWROQ6NTBBB4JWOGWYD6/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WUT5CGHERM6PDXKCM7Z3IJLGIYJ6V6AO/

13. **Oracle Linux**

https://linux.oracle.com/errata/ELSA-2022-1198.html
https://linux.oracle.com/errata/ELSA-2022-9260.html
https://linux.oracle.com/errata/ELSA-2022-9263.html
https://linux.oracle.com/errata/ELSA-2022-9266.html
https://linux.oracle.com/errata/ELSA-2022-9267.html

14. **Pepperl+Fuchs WirelessHART-Gateway**

https://us-cert.cisa.gov/ics/advisories/icsa-22-097-01

15. Red Hat

https://access.redhat.com/errata/RHSA-2022:1103
https://access.redhat.com/errata/RHSA-2022:1173
https://access.redhat.com/errata/RHSA-2022:1174
https://access.redhat.com/errata/RHSA-2022:1185
https://access.redhat.com/errata/RHSA-2022:1186
https://access.redhat.com/errata/RHSA-2022:1198
https://access.redhat.com/errata/RHSA-2022:1199
https://access.redhat.com/errata/RHSA-2022:1209
https://access.redhat.com/errata/RHSA-2022:1213
https://access.redhat.com/errata/RHSA-2022:1253
https://access.redhat.com/errata/RHSA-2022:1254
https://access.redhat.com/errata/RHSA-2022:1263
https://access.redhat.com/errata/RHSA-2022:1264
https://access.redhat.com/errata/RHSA-2022:1275
https://access.redhat.com/errata/RHSA-2022:1276

16. Rockwell Automation ISaGRAF

https://us-cert.cisa.gov/ics/advisories/icsa-22-095-01

17. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.393419
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.408336

18. SonicWall Products

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005

19. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20221072-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221073-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221091-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221093-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221094-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221100-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221102-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221103-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221105-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221108-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221113-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221123-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221127-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221128-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221129-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214936-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214937-1/

20. Ubuntu

https://ubuntu.com/security/notices/USN-5357-2
https://ubuntu.com/security/notices/USN-5358-2
https://ubuntu.com/security/notices/USN-5361-1
https://ubuntu.com/security/notices/USN-5362-1
https://ubuntu.com/security/notices/USN-5364-1
https://ubuntu.com/security/notices/USN-5365-1
https://ubuntu.com/security/notices/USN-5366-1
https://ubuntu.com/security/notices/USN-5368-1
https://ubuntu.com/security/notices/USN-5369-1
https://ubuntu.com/security/notices/USN-5370-1

21. Xen

https://xenbits.xen.org/xsa/advisory-397.html
https://xenbits.xen.org/xsa/advisory-399.html
https://xenbits.xen.org/xsa/advisory-400.html

Sources of product vulnerability information:

Cisco
Citrix
Debian
F5 Products
Fortinet
FreeBSD
Huawei
IBM
openSUSE
Oracle Linux
Red Hat
Slackware
SonicWall
SUSE
Ubuntu
US-CERT
Xen

Contact:

cert@govcert.gov.hk