GovCERT.HK

Weekly IT Security News Bulletin, 2022-W01

3 January – 9 January 2022

Headlines

Google Docs comments weaponised in phishing campaign

- Researchers from a security firm observed that attackers abused the comment feature in Google Docs to spread emails with malicious content to their targets. At least 500 email inboxes, primarily from Outlook users, experienced the email attack.

- By adding a comment to a malicious Google Docs document that assigns a recipient's email address with a symbol "@" in front of it, a system-generated notification email with the content of the document will be issued to the target. Given that the email was sent directly by Google without the presence of the attacker's email address, its legitimacy could help to gain victims' trust and evade detection from anti-spam filters.

- According to the report, the technique of leveraging the comment feature could also be applied in other Google collaboration tools such as Google Slides. The security firm notified Google of the issue in early January.

Advice

- Users should stay extra vigilant against any suspicious emails and do not open attachments or click embedded links unless their authenticity is verified.
- Organisations should regularly provide awareness training to their employees for defending against cyber security attacks.

Sources

- Dark Reading
- Avanan

Risk of copying-pasting commands from webpages

- It is common for system administrators, developers and general users to search for syntax of computing commands from the Internet. However, inadvertently copying-pasting computing commands from webpages directly into a terminal for execution could pose a security risk.

- Security researchers demonstrated that specially crafted JavaScript functions could be used to manipulate user's clipboard content that copied from a webpage and replace with malicious commands. By pasting the clipboard contents to the command console directly, malicious command might be run and executed arbitrary commands.

- Furthermore, although the copy-and-paste function provides a way to save a lot of repetitive effort, the clipboard should not be considered as a secure tool to hold sensitive data in plain text such as a password. Users should make aware that any applications including malware in a system are able to access the clipboard contents directly.

Advice

- Verify the computing commands copied from webpages, such as pasting the copied contents to a plain text editor, before being executed.
- Do not use the copy-and-paste function to handle sensitive information such as user credentials.

Sources

- Wizer
- Bleeping Computer
- NowSecure

Product Vulnerability Notes & Security Updates

1. **Android**

   https://source.android.com/security/bulletin/2022-01-01

2. **CentOS**

   https://lists.centos.org/pipermail/centos-announce/2022-January/073535.html

3. **Debian**

   https://www.debian.org/security/2022/dsa-5035
   https://www.debian.org/security/2022/dsa-5036

4. **F5 Products**

   https://support.f5.com/csp/article/K10396196

5. **Fernhill SCADA**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-006-02

6. **IDEC PLCs**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-006-03

7. **Omron CX-One**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-006-01

8. **openSUSE**

   https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4GRZCYHIJFWN3FE3P7JJYRY7F7UO2HTA/

9. **Oracle Linux**

   https://linux.oracle.com/errata/ELSA-2021-9568.html
   https://linux.oracle.com/errata/ELSA-2021-9638.html
   https://linux.oracle.com/errata/ELSA-2022-0001.html
   https://linux.oracle.com/errata/ELSA-2022-0003.html
   https://linux.oracle.com/errata/ELSA-2022-9005.html

10. **Philips Engage Software**

    https://us-cert.cisa.gov/ics/advisories/icsma-22-006-01

11. Red Hat

https://access.redhat.com/errata/RHSA-2021:5208
https://access.redhat.com/errata/RHSA-2022:0001
https://access.redhat.com/errata/RHSA-2022:0002
https://access.redhat.com/errata/RHSA-2022:0003
https://access.redhat.com/errata/RHSA-2022:0007
https://access.redhat.com/errata/RHSA-2022:0008
https://access.redhat.com/errata/RHSA-2022:0011
https://access.redhat.com/errata/RHSA-2022:0015
https://access.redhat.com/errata/RHSA-2022:0034
https://access.redhat.com/errata/RHSA-2022:0041

12. SonicWall Products

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0027
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0028

13. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220021-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220028-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220029-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220030-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220031-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220032-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220034-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214872-1/

14. Symantec

https://support.broadcom.com/security-advisory/content/security-advisories/Layer7-API-Gateway-Security-Advisory-Log4J-CVE-2021-44228,-CVE-2021-45046,-CVE-2021-4104/SYMSA19791
https://support.broadcom.com/security-advisory/content/security-advisories/Security-Advisory-for-Log4j-vulnerability/SYMSA19795
https://support.broadcom.com/security-advisory/content/security-advisories/Symantec-Security-Advisory-for-Log4j-Vulnerability/SYMSA19793

15. Ubuntu

https://ubuntu.com/security/notices/LSN-0083-1
https://ubuntu.com/security/notices/USN-5204-1
https://ubuntu.com/security/notices/USN-5206-1
https://ubuntu.com/security/notices/USN-5207-1
https://ubuntu.com/security/notices/USN-5208-1
https://ubuntu.com/security/notices/USN-5209-1
https://ubuntu.com/security/notices/USN-5210-1
https://ubuntu.com/security/notices/USN-5211-1
https://ubuntu.com/security/notices/USN-5212-1
https://ubuntu.com/security/notices/USN-5213-1

16. VMware

https://www.vmware.com/security/advisories/VMSA-2022-0001.html

17. WordPress

https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/

Sources of product vulnerability information:

Android
Broadcom
CentOS
Debian
F5 Products
openSUSE
Oracle Linux
Red Hat
SonicWall
SUSE
Ubuntu
US-CERT
VMware
WordPress

Contact:

cert@govcert.gov.hk