GovCERT.HK

Weekly IT Security News Bulletin, 2021-W11
15 March – 21 March 2021

Headlines

Business email compromise attacks on the rise

- The Federal Bureau of Investigation (FBI) of the United States of America published an annual report on cybercrime, revealing an increase in number of business email compromise (BEC) cases which cause loss of more than US$ 1.8 billion in 2020.

- In BEC scams, the attackers compromise business email accounts by social engineering or intrusion for performing unauthorised fund transfers. It is observed that the scammers have taken a more sophisticated approach. In the past, scammers usually launched BEC attacks by first intruding into or spoofing the email accounts of key personnel of organisations and use them to send out fraudulent emails for requesting fund transfer to designated locations. Now the scammers also compromise personal emails and other email accounts (e.g., vendors and lawyers) and adopt different scam schemes like extortion, tech support and romance scams to perform identity theft. In many cases, victims were lured to provide their identities which were then exploited by the scammers to create bank accounts for receiving BEC funds and transferring to crypto-currency accounts.

- The report also highlights tech support fraud as a common scam scheme, in which scammers pretend to be a technical support staff offering assistance to victims to fix issues like compromised accounts and computer virus infection and ask victims to transfer funds to foreign accounts or purchase prepaid cards. The losses in such scam were more than US$146 million.

- To raise awareness of the business sector, FBI has also issued a warning to private companies about the threat of BEC on 17 March 2021.

Advice

- Verify the senders of emails, especially those requesting recipients to provide identity information or perform funds transfer.
- Report any fraud recognised to the financial institutions and request cancellation or reversal of any unauthorised transactions as soon as possible.

Sources

- FBI
- Dark Reading
- Bleeping Computer

Proof-of-concept of Spectre exploit on browsers

- While three years have gone by since the Spectre vulnerability was first discovered in 2018, Google has recently released proof-of-concept for launching Spectre attack on Chrome browser.

- Spectre is a vulnerability in processors which allows attackers to take a peek on private data in memory by launching side-channel attack through analysis of the speculative execution of instructions by processors. While hardware and software manufacturers like Intel and Microsoft have released fixes to mitigate the vulnerability, the PoC developed by Google shows that Spectre can still be exploited to launch attack on Javascript engines. This can result in leakage of sensitive information like passwords stored in browsers.

- The PoC shows that the existing mitigation measure (reduction of timer granularity) cannot effectively stop attackers from measuring the access time to data. By abusing the cache algorithm (Tree-PLRU) used in processors, hackers can amplify the cache timing so as to determine information being read from cache. In the demonstration, the code allows data to be extracted from memory at speed of one kilobyte per second. While Google researchers commented that the PoC could not be re-used for malicious purposes without significant modifications, they believed that the code could work on different CPUs and operating systems.

- To identify any application resources which are not covered by the default protection from Google Chrome and are therefore subject to Spectre vulnerability, Google has developed a Chrome extension tool for web developers to scan their web applications.

Advice

- Deploy proper web isolation through security mechanisms like cross-origin resource policy and fetch metadata request headers to avoid access to cross-origin resources on browsers.
- Regularly review the security of websites and applications and apply vulnerability patching in a timely manner.

Sources

- Google
- Threatpost
- Security Affairs

Product Vulnerability Notes & Security Updates

1. **Cisco Products**

   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-132w134w-overflow-Pptt4H2p

2. **Debian**

   https://www.debian.org/security/2021/dsa-4868
   https://www.debian.org/security/2021/dsa-4869
   https://www.debian.org/security/2021/dsa-4870
   https://www.debian.org/security/2021/dsa-4871

3. **F5 Traffix SDC**

   https://support.f5.com/csp/article/K00174195
   https://support.f5.com/csp/article/K73648110

4. **GE UR family**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-075-02

5. **Hitachi ABB Power Grids eSOMS**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-077-02
   https://us-cert.cisa.gov/ics/advisories/icsa-21-077-03

6. **Microsoft Edge (Chromium based)**

   https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#march-13-2021

7. **Oracle Linux**

   https://linux.oracle.com/errata/ELSA-2021-0851.html
   https://linux.oracle.com/errata/ELSA-2021-0856.html
   https://linux.oracle.com/errata/ELSA-2021-9107.html
   https://linux.oracle.com/errata/ELSA-2021-9109.html
   https://linux.oracle.com/errata/ELSA-2021-9112.html
   https://linux.oracle.com/errata/ELSA-2021-9113.html
   https://linux.oracle.com/errata/ELSA-2021-9114.html
   https://linux.oracle.com/errata/ELSA-2021-9115.html
   https://linux.oracle.com/errata/ELSA-2021-9116.html

8. Red Hat

https://access.redhat.com/errata/RHSA-2021:0816
https://access.redhat.com/errata/RHSA-2021:0818
https://access.redhat.com/errata/RHSA-2021:0819
https://access.redhat.com/errata/RHSA-2021:0827
https://access.redhat.com/errata/RHSA-2021:0830
https://access.redhat.com/errata/RHSA-2021:0831
https://access.redhat.com/errata/RHSA-2021:0834
https://access.redhat.com/errata/RHSA-2021:0835
https://access.redhat.com/errata/RHSA-2021:0837
https://access.redhat.com/errata/RHSA-2021:0848
https://access.redhat.com/errata/RHSA-2021:0851
https://access.redhat.com/errata/RHSA-2021:0856
https://access.redhat.com/errata/RHSA-2021:0857
https://access.redhat.com/errata/RHSA-2021:0860
https://access.redhat.com/errata/RHSA-2021:0862
https://access.redhat.com/errata/RHSA-2021:0871
https://access.redhat.com/errata/RHSA-2021:0872
https://access.redhat.com/errata/RHSA-2021:0873
https://access.redhat.com/errata/RHSA-2021:0874
https://access.redhat.com/errata/RHSA-2021:0876
https://access.redhat.com/errata/RHSA-2021:0877
https://access.redhat.com/errata/RHSA-2021:0878
https://access.redhat.com/errata/RHSA-2021:0881
https://access.redhat.com/errata/RHSA-2021:0882
https://access.redhat.com/errata/RHSA-2021:0883
https://access.redhat.com/errata/RHSA-2021:0885
https://access.redhat.com/errata/RHSA-2021:0915
https://access.redhat.com/errata/RHSA-2021:0916
https://access.redhat.com/errata/RHSA-2021:0922
https://access.redhat.com/errata/RHSA-2021:0931
https://access.redhat.com/errata/RHSA-2021:0933
https://access.redhat.com/errata/RHSA-2021:0934
https://access.redhat.com/errata/RHSA-2021:0937
https://access.redhat.com/errata/RHSA-2021:0940

9. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.436701
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.657570

10. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210772-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210773-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210776-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210777-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210778-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210779-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210781-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210782-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210793-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210794-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210800-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210801-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210806-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210808-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210809-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210818-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210823-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210826-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210835-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210840-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210841-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210842-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210849-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210853-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210859-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210864-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210868-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210869-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210870-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114667-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114668-1/

11. Symantec Management Center (MC)

https://support.broadcom.com/security-advisory/content/security-advisories/Apache-Tomcat-Vulnerabilities-May-2020-Mar-2021/SYMSA17650

12. Ubuntu

https://ubuntu.com/security/notices/USN-4754-3
https://ubuntu.com/security/notices/USN-4764-1
https://ubuntu.com/security/notices/USN-4876-1
https://ubuntu.com/security/notices/USN-4877-1
https://ubuntu.com/security/notices/USN-4878-1
https://ubuntu.com/security/notices/USN-4879-1
https://ubuntu.com/security/notices/USN-4880-1
https://ubuntu.com/security/notices/USN-4881-1
https://ubuntu.com/security/notices/USN-4882-1

13. Xen

https://xenbits.xen.org/xsa/advisory-368.html

Sources of product vulnerability information:

Broadcom
Cisco
Debian
F5
Microsoft
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
US-CERT
Xen

Contact:

cert@govcert.gov.hk