GovCERT.HK

Weekly IT Security News Bulletin, 2021-W05

1 February – 7 February 2021

Headlines

Be aware of suspicious browser extension

- A popular browser extension called "The Great Suspender" was found malicious and disabled by Google. The extension has once been the most popular extension of such kind with more than 2 million downloads on Chrome Web Store. It is widely used to minimise the memory footprint of Chrome web browser by suspending tabs which are not in use for a while.

- The original developer of the browser extension previously sold it to another unknown party who then quietly inserted suspicious Open Web Analytics tracker code into the extension for tracking and advertising fraud, submitted the code changes to GitHub repository and released it through Chrome Web Store. It was also found that the extension may also connect to other servers and execute code from them. Some users reported that some of the extension code can possibly be linked to malware and crypto-mining.

- As warned by security researchers, the extension can potentially allow code execution from untrusted third-parties and modification of websites viewed on the browsers. In view of the potential threat to the users, Microsoft had also labelled the browser extension as containing malware.

Advice

- Do not install browser extension from untrusted source.
- Stay alerted on any news and updates on extensions in use for any security issues or transfer of ownership to untrusted third parties.
- Review the version updates and check for any suspicious code changes made.

Sources

- GitHub
- The Register
- The Hacker News

Exploiting Plex media servers for DDoS attacks

- Plex, a media player system and software suite usually shipped with network attached storage (NAS) devices, was found to be exploited for launching distributed denial of service (DDoS) attacks.

- When a Plex media server is up and running, it will perform scanning for other devices on the local network by making Simple Service Discovery Protocol (SSDP) probe. However, once the server finds a local router supporting SSDP, it will add a NAT forwarding rule to the router and expose its service on the internet on a designated port. Given that SSDP protocol can be used as a vector for reflection/amplification DDoS attack with an amplification factor of 4.7, attackers may scan the internet for Plex servers with designated port opened and exploit them for DDoS attacks.

- A study conducted by a security vendor identified about 37,000 Plex servers on the Internet which can be potentially abused, where 15,000 distinct entities have already been exploited for SSDP DDoS attacks. Plex is still working on a patch to resolve the issue.

Advice

- Do not exposure unnecessary ports or services to the Internet.
- Disable port-forwarding rules if not needed.
- Disable unnecessary services and protocols on NAS devices to prevent abuse.

Sources

- Netscout
- ZDNet

Product Vulnerability Notes & Security Updates

1. Android

https://source.android.com/security/bulletin/2021-02-01

2. Apple Products

https://support.apple.com/en-us/HT212147
https://support.apple.com/en-us/HT212152

3. CentOS

https://lists.centos.org/pipermail/centos-announce/2021-February/048257.html
https://lists.centos.org/pipermail/centos-announce/2021-February/048259.html
https://lists.centos.org/pipermail/centos-announce/2021-February/048262.html
https://lists.centos.org/pipermail/centos-announce/2021-February/048265.html

4. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-infodisc-4mtm9Gyt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dos-WwDdghs2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pe-QpzCAePe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-msx-dos-4j7sytvU
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-7MKrW7Nq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sudo-privesc-jan2021-qnYQfcM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-invcert-eOpRvCKH
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-linkinj-WWZpVqu9
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K

5. Debian

https://www.debian.org/security/2021/dsa-4843
https://www.debian.org/security/2021/dsa-4844
https://www.debian.org/security/2021/dsa-4845

6. F5 Products

https://support.f5.com/csp/article/K58149033
https://support.f5.com/csp/article/K84900646
https://support.f5.com/csp/article/K86488846

7. Fortinet Products

https://www.fortiguard.com/psirt/FG-IR-20-122
https://www.fortiguard.com/psirt/FG-IR-20-229
https://www.fortiguard.com/psirt/FG-IR-20-232

8. FreeBSD

https://www.freebsd.org/security/advisories/FreeBSD-SA-21:01.fsdisclosure.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-21:02.xenoom.asc

9. Gentoo Linux

https://security.gentoo.org/glsa/202102-01

10. Google Chrome

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html

11. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-cgp-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-csvinjection-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210203-01-informationleak-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210203-01-manageone-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210203-01-plaintextlog-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210203-01-resourcemanagement-en

12. IBM InfoSphere Information Server

https://www.ibm.com/support/pages/node/6409184

13. Oracle Products

https://linux.oracle.com/errata/ELSA-2021-0304.html
https://linux.oracle.com/errata/ELSA-2021-0336.html
https://linux.oracle.com/errata/ELSA-2021-0343.html
https://linux.oracle.com/errata/ELSA-2021-0347.html
https://linux.oracle.com/errata/ELSA-2021-0348.html
https://linux.oracle.com/errata/ELSA-2021-0411.html
https://linux.oracle.com/errata/ELSA-2021-9023.html
https://linux.oracle.com/errata/ELSA-2021-9024.html
https://linux.oracle.com/errata/ELSA-2021-9025.html
https://linux.oracle.com/errata/ELSA-2021-9030.html

14. Red Hat

https://access.redhat.com/errata/RHSA-2021:0281
https://access.redhat.com/errata/RHSA-2021:0282
https://access.redhat.com/errata/RHSA-2021:0292
https://access.redhat.com/errata/RHSA-2021:0304
https://access.redhat.com/errata/RHSA-2021:0306
https://access.redhat.com/errata/RHSA-2021:0307
https://access.redhat.com/errata/RHSA-2021:0317
https://access.redhat.com/errata/RHSA-2021:0318
https://access.redhat.com/errata/RHSA-2021:0319
https://access.redhat.com/errata/RHSA-2021:0320
https://access.redhat.com/errata/RHSA-2021:0327
https://access.redhat.com/errata/RHSA-2021:0329
https://access.redhat.com/errata/RHSA-2021:0336
https://access.redhat.com/errata/RHSA-2021:0338
https://access.redhat.com/errata/RHSA-2021:0339
https://access.redhat.com/errata/RHSA-2021:0346
https://access.redhat.com/errata/RHSA-2021:0354
https://access.redhat.com/errata/RHSA-2021:0384
https://access.redhat.com/errata/RHSA-2021:0395
https://access.redhat.com/errata/RHSA-2021:0401
https://access.redhat.com/errata/RHSA-2021:0411
https://access.redhat.com/errata/RHSA-2021:0417
https://access.redhat.com/errata/RHSA-2021:0420
https://access.redhat.com/errata/RHSA-2021:0421

15. Rockwell Automation MicroLogix 1400

https://us-cert.cisa.gov/ics/advisories/icsa-21-033-01

16. Siemens SIMATIC HMI Comfort Panels & SIMATIC HMI KTP Mobile Panels

https://us-cert.cisa.gov/ics/advisories/icsa-21-033-02

17. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210241-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210243-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210246-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210251-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210258-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210259-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210263-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210275-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210276-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210277-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210284-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210285-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210286-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210297-1
https://www.suse.com/support/update/announcement/2021/suse-su-20210298-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210299-1/

https://www.suse.com/support/update/announcement/2021/suse-su-20210300-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114609-1/

18. Ubuntu

https://ubuntu.com/security/notices/USN-4467-2
https://ubuntu.com/security/notices/USN-4709-1
https://ubuntu.com/security/notices/USN-4710-1
https://ubuntu.com/security/notices/USN-4711-1
https://ubuntu.com/security/notices/USN-4712-1
https://ubuntu.com/security/notices/USN-4713-1
https://ubuntu.com/security/notices/USN-4715-1
https://ubuntu.com/security/notices/USN-4715-2
https://ubuntu.com/security/notices/USN-4716-1
https://ubuntu.com/security/notices/USN-4717-1
https://ubuntu.com/security/notices/USN-4718-1
https://ubuntu.com/security/notices/USN-4719-1
https://ubuntu.com/security/notices/USN-4720-1
https://ubuntu.com/security/notices/USN-4720-2
https://ubuntu.com/security/notices/USN-4721-1
https://ubuntu.com/security/notices/USN-4722-1

19. Wireshark

https://www.wireshark.org/security/wnpa-sec-2021-01.html
https://www.wireshark.org/security/wnpa-sec-2021-02.html

Sources of product vulnerability information:

Android
Apple
CentOS
Cisco
Debian
F5
Fortinet
FreeBSD
Gentoo Linux
Google Chrome
Huawei
IBM
Oracle Linux
Red Hat
SUSE
Ubuntu
US-CERT
Wireshark

Contact:

cert@govcert.gov.hk