GovCERT.HK

Weekly IT Security News Bulletin, 2021-W04

25 January – 31 January 2021

Headlines

Zero-day vulnerabilities fixed in Apple products

- Apple released security update to fix three zero-day vulnerabilities found in the iOS kernel and WebKit browser engine. The vulnerabilities have been actively exploited in the wild and can lead to privilege elevation and arbitrary code execution.
- While Apple has not disclosed much details about how the vulnerabilities have been exploited, it is believed that malicious actors can make use of them to compromise target devices by launching watering hole attacks through malicious websites.
- At the same time, a security researcher discovered that some mitigation measures were adopted in the latest iOS version to fix the zero-click flaw in Apple iMessage instant messaging client which allows attackers to circumvent security protections through memory corruption. The flaw was believed to be linked to a notable cyberespionage campaign in Middle East.
- A new sandbox service is introduced to iOS to allow code to be executed in an environment isolated from the rest of the operating system. It handles the parsing and inspection of untrusted data in inbound iMessages in a sandbox environment so as to forbid any malicious code hidden in the message from accessing the operating system or data and safeguard the device from memory corruption.

Advice

- Apply security patch on operating systems in a timely manner.
- Configure browsers to alert about malicious websites.
- Monitor network traffic for any access to malicious websites.
- Do not open untrusted links or attachments in email or messages.

Sources

- Threatpost
- Hacker News
- Project Zero
- ZDnet

Gain root privilege through vulnerability in Sudo

- A security researcher found a severe vulnerability, named as "Baron Samedit" (CVE-2021-3156), in sudo, which is a utility available in almost every Unix and Linux based operating systems.

- System administrators use sudo to delegate root authority to specific users and allow the users to execute programs with privileges of other users. However, it is found that sudo improperly parses the command line parameter and this can lead to heap-based buffer overflow. By exploiting the buffer overflow flaw, unprivileged local users can invoke sudoedit command with specifically crafted parameters in shell mode and obtain full root privileges on the affected operating systems, even if they are not on the sudoer list.

- However, the vulnerability cannot be remotely exploited and the malicious actors still need to have direct access to the vulnerable systems or get remote access to them through other loopholes.

- The author of sudo was informed about vulnerability and has released a patched update to fix it. Administrators of Unix and Linux distributions with sudo should apply patches or update from the respective vendor so as to upgrade sudo to the latest version.

Advice

- Apply patch and security update to operating systems in a timely manner.
- Disable sudo if it is not in use.
- Use containers or virtual machines to provide additional layer of isolation and security to the underlying host.

Sources

- Qualys
- Threatpost
- Dark Reading

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/zh-tw/HT212145
https://support.apple.com/zh-tw/HT212153

2. CentOS

https://lists.centos.org/pipermail/centos-announce/2021-January/048249.html
https://lists.centos.org/pipermail/centos-announce/2021-January/048250.html
https://lists.centos.org/pipermail/centos-announce/2021-January/048251.html
https://lists.centos.org/pipermail/centos-announce/2021-January/048252.html

3. Debian

https://www.debian.org/security/2021/dsa-4834
https://www.debian.org/security/2021/dsa-4835
https://www.debian.org/security/2021/dsa-4836
https://www.debian.org/security/2021/dsa-4837
https://www.debian.org/security/2021/dsa-4838
https://www.debian.org/security/2021/dsa-4839
https://www.debian.org/security/2021/dsa-4840
https://www.debian.org/security/2021/dsa-4841

4. Fuji Electric Tellus Lite V-Simulator and V-Server Lite

https://us-cert.cisa.gov/ics/advisories/icsa-21-026-01

5. Gentoo Linux

https://security.gentoo.org/glsa/202101-12
https://security.gentoo.org/glsa/202101-13
https://security.gentoo.org/glsa/202101-15
https://security.gentoo.org/glsa/202101-16
https://security.gentoo.org/glsa/202101-17
https://security.gentoo.org/glsa/202101-18
https://security.gentoo.org/glsa/202101-19
https://security.gentoo.org/glsa/202101-20
https://security.gentoo.org/glsa/202101-21
https://security.gentoo.org/glsa/202101-22
https://security.gentoo.org/glsa/202101-23
https://security.gentoo.org/glsa/202101-24
https://security.gentoo.org/glsa/202101-25
https://security.gentoo.org/glsa/202101-26
https://security.gentoo.org/glsa/202101-27
https://security.gentoo.org/glsa/202101-28
https://security.gentoo.org/glsa/202101-29
https://security.gentoo.org/glsa/202101-30
https://security.gentoo.org/glsa/202101-31
https://security.gentoo.org/glsa/202101-32
https://security.gentoo.org/glsa/202101-33

https://security.gentoo.org/glsa/202101-34
https://security.gentoo.org/glsa/202101-35
https://security.gentoo.org/glsa/202101-36
https://security.gentoo.org/glsa/202101-37
https://security.gentoo.org/glsa/202101-38

6. IBM Products

https://www.ibm.com/support/pages/node/6408244
https://www.ibm.com/support/pages/node/6409184

7. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-0218.html
https://linux.oracle.com/errata/ELSA-2021-0221.html
https://linux.oracle.com/errata/ELSA-2021-0288.html
https://linux.oracle.com/errata/ELSA-2021-0290.html
https://linux.oracle.com/errata/ELSA-2021-9019.html

8. Red Hat

https://access.redhat.com/errata/RHSA-2021:0171
https://access.redhat.com/errata/RHSA-2021:0172
https://access.redhat.com/errata/RHSA-2021:0218
https://access.redhat.com/errata/RHSA-2021:0219
https://access.redhat.com/errata/RHSA-2021:0220
https://access.redhat.com/errata/RHSA-2021:0221
https://access.redhat.com/errata/RHSA-2021:0222
https://access.redhat.com/errata/RHSA-2021:0223
https://access.redhat.com/errata/RHSA-2021:0224
https://access.redhat.com/errata/RHSA-2021:0225
https://access.redhat.com/errata/RHSA-2021:0226
https://access.redhat.com/errata/RHSA-2021:0227
https://access.redhat.com/errata/RHSA-2021:0240
https://access.redhat.com/errata/RHSA-2021:0245
https://access.redhat.com/errata/RHSA-2021:0246
https://access.redhat.com/errata/RHSA-2021:0247
https://access.redhat.com/errata/RHSA-2021:0248
https://access.redhat.com/errata/RHSA-2021:0250
https://access.redhat.com/errata/RHSA-2021:0257
https://access.redhat.com/errata/RHSA-2021:0258
https://access.redhat.com/errata/RHSA-2021:0266
https://access.redhat.com/errata/RHSA-2021:0285
https://access.redhat.com/errata/RHSA-2021:0288
https://access.redhat.com/errata/RHSA-2021:0289
https://access.redhat.com/errata/RHSA-2021:0290

9. Rockwell Automation FactoryTalk Linx and FactoryTalk Services Platform

https://us-cert.cisa.gov/ics/advisories/icsa-21-028-01

10. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.343320
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.461226

11. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210192-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210194-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210195-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210196-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210197-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210198-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210199-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210200-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210210-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210217-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210222-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210223-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210224-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210225-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210226-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210227-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210232-1/

12. Trend Micro Products

https://success.trendmicro.com/solution/000284202
https://success.trendmicro.com/solution/000284205
https://success.trendmicro.com/solution/000284206
https://success.trendmicro.com/solution/000284207

13. Ubuntu

https://ubuntu.com/security/notices/USN-4702-1
https://ubuntu.com/security/notices/USN-4703-1
https://ubuntu.com/security/notices/USN-4704-1
https://ubuntu.com/security/notices/USN-4705-1
https://ubuntu.com/security/notices/USN-4705-2
https://ubuntu.com/security/notices/USN-4706-1
https://ubuntu.com/security/notices/USN-4707-1
https://ubuntu.com/security/notices/USN-4708-1
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-4714-1

14. Xen

https://xenbits.xen.org/xsa/advisory-360.html

Sources of product vulnerability information:

Apple
CentOS
Debian
Gentoo Linux
IBM
Oracle Linux
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
US-CERT
Xen

Contact:

cert@govcert.gov.hk