GovCERT.HK

Weekly IT Security News Bulletin, 2020-W50

7 December – 13 December 2020

Headlines

Video conferencing tool vulnerable to remote code execution

- Cisco Jabber, a video conferencing and messaging tool, was found to be susceptible to arbitrary code execution, due to a flaw in message content validation which allows cross-site scripting to bypass the sandbox in the browser for preventing unauthorised file access.

- An attacker can exploit the vulnerability to remotely execute code on the target's system with the privilege of the victim's account running the tool by sending a specially crafted message. The whole process does not require any user interaction, and malicious payloads can be further spread out through instant messages. Depending on the privileges granted to the users, the vulnerability can allow program installation and tampering or theft of data. The impact to the victim's system will be less if the users and application are granted with fewer privileges.

- The vendor has already released a patch to fix this critical vulnerability (CVE-2020-26085) on 10 December 2020.

Advice

- Apply the latest patches to video conferencing tools.
- Do not open messages or follow links from untrusted parties.
- Only grant privileges to users and applications on a need basis.

Sources

- Watchcom
- Threatpost
- The Hacker News

Enforcing DMARC to protect domains against email spoofing

- Researchers recently observed a global spear-phishing campaign targeting users of the Microsoft Office 365 from various sectors like finance and health care, and revealed that Microsoft failed to enforce Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect their domain.

- The attackers sent phishing emails to victims pretending to be from Microsoft to invite them to use the new feature of checking quarantined messages. Victims were asked to click on a link which redirected them to a fake security portal in which they were asked to enter the login credentials for their Office 365 accounts.

- In this spear-phishing attack, the attackers were able to mimic the legitimate domain of Microsoft. Microsoft failed to block such emails from the fraudulent senders and stop such spoofing with DMARC, which is a protocol to protect domains from being spoofed.

- Microsoft replied that they have performed DMARC checks on the emails but users may choose to override or disable the controls. Instead of blocking those emails failing the DMARC checks, Microsoft may quarantine the emails or label them as spam, depending on the users' security settings.

Advice

- Adopt DMARC to protect against domain spoofing and reject any emails fraudulent domains at the email gateway.
- Do not open spam mails failing the DMARC check.
- Educate users to be aware of phishing emails and do not follow any links embedded in emails from untrusted sources.

Sources

- Ironscales
- Help Net Security
- SC Media

Product Vulnerability Notes & Security Updates

1. Android

https://source.android.com/security/bulletin/2020-12-01

2. CentOS

https://lists.centos.org/pipermail/centos-announce/2020-December/048209.html

3. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-ZktzjpgO

4. Citrix Secure Mail

https://support.citrix.com/article/CTX286763

5. Debian

https://www.debian.org/security/2020/dsa-4803
https://www.debian.org/security/2020/dsa-4804
https://www.debian.org/security/2020/dsa-4805
https://www.debian.org/security/2020/dsa-4806
https://www.debian.org/security/2020/dsa-4807
https://www.debian.org/security/2020/dsa-4808
https://www.debian.org/security/2020/dsa-4809

6. F5 Products

https://support.f5.com/csp/article/K04337834
https://support.f5.com/csp/article/K05204103
https://support.f5.com/csp/article/K07020416
https://support.f5.com/csp/article/K20984059
https://support.f5.com/csp/article/K37960100
https://support.f5.com/csp/article/K42202505
https://support.f5.com/csp/article/K42696541
https://support.f5.com/csp/article/K43530108
https://support.f5.com/csp/article/K70117303
https://support.f5.com/csp/article/K83102920
https://support.f5.com/csp/article/K92451315

7. FreeBSD

https://www.freebsd.org/security/advisories/FreeBSD-SA-20:33.openssl.asc

8. GE Healthcare Imaging and Ultrasound Products

https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01

9. **Gentoo Linux**

https://security.gentoo.org/glsa/202012-01
https://security.gentoo.org/glsa/202012-02
https://security.gentoo.org/glsa/202012-03
https://security.gentoo.org/glsa/202012-05
https://security.gentoo.org/glsa/202012-06
https://security.gentoo.org/glsa/202012-07
https://security.gentoo.org/glsa/202012-08

10. **Host Engineering H2-ECOM100 Module**

https://us-cert.cisa.gov/ics/advisories/icsa-20-345-02

11. **Huawei Products**

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201209-01-csvinjection-en

12. **IBM Products**

https://www.ibm.com/support/pages/node/6379260
https://www.ibm.com/support/pages/node/6380430

13. **McAfee Products**

https://kc.mcafee.com/corporate/index?page=content&id=SB10338
https://kc.mcafee.com/corporate/index?page=content&id=SB10340

14. **Medtronic MyCareLink Smart**

https://us-cert.cisa.gov/ics/advisories/icsma-20-345-01

15. **Mitsubishi Electric GOT and Tension Controller**

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-02

16. **Multiple Embedded TCP/IP Stacks**

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01

17. **Oracle Linux**

https://linux.oracle.com/errata/ELSA-2020-5350.html
https://linux.oracle.com/errata/ELSA-2020-5966.html
https://linux.oracle.com/errata/ELSA-2020-5968.html
https://linux.oracle.com/errata/ELSA-2020-5983.html

18. QNAP Products

https://www.qnap.com/en/security-advisory/qsa-20-12
https://www.qnap.com/en/security-advisory/qsa-20-13
https://www.qnap.com/en/security-advisory/qsa-20-14
https://www.qnap.com/en/security-advisory/qsa-20-15
https://www.qnap.com/en/security-advisory/qsa-20-16

19. Red Hat

https://access.redhat.com/errata/RHSA-2020:5350
https://access.redhat.com/errata/RHSA-2020:5351
https://access.redhat.com/errata/RHSA-2020:5352
https://access.redhat.com/errata/RHSA-2020:5365
https://access.redhat.com/errata/RHSA-2020:5369
https://access.redhat.com/errata/RHSA-2020:5372
https://access.redhat.com/errata/RHSA-2020:5374
https://access.redhat.com/errata/RHSA-2020:5379

20. Schneider Electric Products

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-03
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-04

21. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-06
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-07
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-08
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-09
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-10

22. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.343700
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.431010

23. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20203624-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203625-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203627-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203628-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203629-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203630-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203631-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203632-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203648-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203651-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203653-1/

https://www.suse.com/support/update/announcement/2020/suse-su-20203656-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203670-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203690-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203698-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203705-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203713-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203714-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203715-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203717-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203718-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203720-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203721-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203722-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203723-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203729-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203732-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203733-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203735-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203736-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203737-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203739-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203740-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203742-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203748-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203749-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014557-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014560-1/

24. Symantec Messaging Gateway

https://support.broadcom.com/security-advisory/content/security-advisories/Privilege-Escalation-and-Information-Disclosure-Vulnerabilities-in-SMG/SYMSA16609

25. Ubuntu

https://ubuntu.com/security/notices/USN-4656-2
https://ubuntu.com/security/notices/USN-4662-1
https://ubuntu.com/security/notices/USN-4663-1
https://ubuntu.com/security/notices/USN-4664-1
https://ubuntu.com/security/notices/USN-4665-1
https://ubuntu.com/security/notices/USN-4665-2
https://ubuntu.com/security/notices/USN-4666-1
https://ubuntu.com/security/notices/USN-4667-1
https://ubuntu.com/security/notices/USN-4668-1
https://ubuntu.com/security/notices/USN-4668-2
https://ubuntu.com/security/notices/USN-4669-1

Sources of product vulnerability information:

- Android
- Broadcom
- CentOS
- Cisco
- Citrix
- Debian
- F5
- FreeBSD
- Gentoo Linux
- Huawei
- IBM
- McAfee
- Oracle Linux
- QNAP
- Red Hat
- Slackware
- SUSE
- Ubuntu
- US-CERT

Contact:

cert@govcert.gov.hk