GovCERT.HK

Weekly IT Security News Bulletin, 2021-W09

1 March – 7 March 2021

Headlines

Patch your Microsoft Exchange server now

- In early March 2021, Microsoft reported that active exploitation of four zero-day vulnerabilities in Microsoft Exchange server was observed. Successful exploitation of the vulnerabilities could allow a remote attacker to access files and mailboxes and install malware on those compromised servers. According to Microsoft, the exploits would affect on-premises version of Exchange server but not the cloud-based version or Exchange online.

- In order to compromise the Exchange servers through the vulnerabilities, the attacker would attempt to make an untrusted connection to the vulnerable Microsoft Exchange Server via port 443. Once connected successfully, the attacker would then exploit one of the four vulnerabilities (identified as CVE-2021-26855) to authenticate as an Exchange server. Such vulnerability can create an attack chain together with the other three vulnerabilities that results in gaining remote access to the vulnerable server.

- Microsoft has released the out-of-band or adhoc patches to fix the vulnerabilities on 2 March 2021. Microsoft also published an advisory for organisations to check if their servers might be compromised.

Advice

- Install security patch immediately on the affected Exchange servers.
- Monitor the network traffic for anomalous conditions and review log files in the Exchange servers to determine if there is any exploitation activity.
- Restrict web access to the Exchange Server by whitelisting only trusted or internal IP addresses if the patch cannot be applied promptly.

Sources

- Microsoft
- US-CERT
- Securelist

Boost digital security with Zero Trust

- Traditional perimeter-based network defense may not be sufficient to protect information system and assets against emerging threats. Following the recent supply-chain attack on the SolarWinds software, the U.S. National Security Agency (NSA) and Microsoft recommend organisations adopting the Zero Trust security model to enhance the security level of their critical networks.

- Zero Trust aims to eliminate implicit trust from the network and always requires continuous verification for any access to resources on a network. Adoption of the principle of the least privileges, continuous monitoring for suspicious activity, and use of multi-factor authentication of users are recommended for a Zero Trust environment.

- Under a Zero Trust architecture, every device is protected by a deny-by-default security policy, thereby blocking unauthorised access requests from/to the device or an application. Organisations are recommended to incorporate Zero Trust concepts into their networks to improve their overall cybersecurity posture.

Advice

- Consider adopting a Zero Trust approach to secure access to critical network infrastructures.
- Grant users with least privilege and access right on a need basis.
- Establish continuous monitoring mechanism for configuration changes, resource accesses, and network traffic for suspicious activity.

Sources

- U.S. National Security Agency
- ITProPortal
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. Android

https://source.android.com/security/bulletin/2021-03-01

2. CentOS

https://lists.centos.org/pipermail/centos-announce/2021-February/048275.html
https://lists.centos.org/pipermail/centos-announce/2021-February/048276.html
https://lists.centos.org/pipermail/centos-announce/2021-February/048277.html
https://lists.centos.org/pipermail/centos-announce/2021-February/048279.html
https://lists.centos.org/pipermail/centos-announce/2021-March/048281.html

3. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-info-disclo-VOu2GHbZ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-rce-dos-U2PsSkz3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-dZRQE8Lc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-sqlinj-HDJUeEAX
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-vman-kth3c82B
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-sigverbypass-gPYXd6Mk
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vdaemon-bo-RuzzEA2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanvman-infodis1-YuQScHB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-ethernet-dos-HGXgJH8n
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-ipsecmgr-dos-3gkHXwvS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-authorization-b-GUEpSLK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-dir-trav-Bpwc5gtm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-distupd-N87eB6Z3

4. Debian

https://www.debian.org/security/2021/dsa-4864
https://www.debian.org/security/2021/dsa-4865
https://www.debian.org/security/2021/dsa-4867

5. F5 Traffix SDC

https://support.f5.com/csp/article/K04553557

6. **Fortinet Products**

https://www.fortiguard.com/psirt/FG-IR-20-224
https://www.fortiguard.com/psirt/FG-IR-20-230
https://www.fortiguard.com/psirt/FG-IR-20-235
https://www.fortiguard.com/psirt/FG-IR-20-236

7. **Joolma!**

https://www.joomla.org/announcements/release-news/5834-joomla-3-9-25.html

8. **MB connect line mbCONNECT24, mymbCONNECT24**

https://us-cert.cisa.gov/ics/advisories/icsa-21-061-03

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

https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#march-4-2021

10. **Oracle Linux**

https://linux.oracle.com/errata/ELSA-2021-0670.html
https://linux.oracle.com/errata/ELSA-2021-0671.html
https://linux.oracle.com/errata/ELSA-2021-0699.html
https://linux.oracle.com/errata/ELSA-2021-9076.html
https://linux.oracle.com/errata/ELSA-2021-9077.html
https://linux.oracle.com/errata/ELSA-2021-9079.html

11. **Red Hat**

https://access.redhat.com/errata/RHSA-2021:0428
https://access.redhat.com/errata/RHSA-2021:0429
https://access.redhat.com/errata/RHSA-2021:0637
https://access.redhat.com/errata/RHSA-2021:0669
https://access.redhat.com/errata/RHSA-2021:0670
https://access.redhat.com/errata/RHSA-2021:0671
https://access.redhat.com/errata/RHSA-2021:0672
https://access.redhat.com/errata/RHSA-2021:0681
https://access.redhat.com/errata/RHSA-2021:0686
https://access.redhat.com/errata/RHSA-2021:0689
https://access.redhat.com/errata/RHSA-2021:0691
https://access.redhat.com/errata/RHSA-2021:0692
https://access.redhat.com/errata/RHSA-2021:0693
https://access.redhat.com/errata/RHSA-2021:0694
https://access.redhat.com/errata/RHSA-2021:0696
https://access.redhat.com/errata/RHSA-2021:0697
https://access.redhat.com/errata/RHSA-2021:0698
https://access.redhat.com/errata/RHSA-2021:0699
https://access.redhat.com/errata/RHSA-2021:0700
https://access.redhat.com/errata/RHSA-2021:0701
https://access.redhat.com/errata/RHSA-2021:0702
https://access.redhat.com/errata/RHSA-2021:0703
https://access.redhat.com/errata/RHSA-2021:0704

https://access.redhat.com/errata/RHSA-2021:0705
https://access.redhat.com/errata/RHSA-2021:0706
https://access.redhat.com/errata/RHSA-2021:0710
https://access.redhat.com/errata/RHSA-2021:0711
https://access.redhat.com/errata/RHSA-2021:0717
https://access.redhat.com/errata/RHSA-2021:0719
https://access.redhat.com/errata/RHSA-2021:0727
https://access.redhat.com/errata/RHSA-2021:0733
https://access.redhat.com/errata/RHSA-2021:0734
https://access.redhat.com/errata/RHSA-2021:0735
https://access.redhat.com/errata/RHSA-2021:0736

12. Rockwell Automation 1734-AENTR Series B and Series C

https://us-cert.cisa.gov/ics/advisories/icsa-21-063-01

13. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20202173-2/
https://www.suse.com/support/update/announcement/2021/suse-su-20210619-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210624-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210625-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210626-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210627-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210628-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210630-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210631-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210647-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210648-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210649-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210650-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210651-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210652-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210653-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210654-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210658-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210659-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210663-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210664-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210665-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210667-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210668-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210669-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210670-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210673-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210674-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210675-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210676-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210679-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210682-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210683-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210684-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210685-1/

https://www.suse.com/support/update/announcement/2021/suse-su-20210686-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210687-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210689-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210692-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210693-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210694-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210695-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210696-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210713-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210714-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114646-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114647-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114649-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114650-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114657-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114659-1/

14. Trend Micro Products

https://success.trendmicro.com/solution/000285675

15. Ubuntu

https://ubuntu.com/security/notices/USN-4737-2
https://ubuntu.com/security/notices/USN-4754-4
https://ubuntu.com/security/notices/USN-4756-1
https://ubuntu.com/security/notices/USN-4757-1
https://ubuntu.com/security/notices/USN-4757-2

Sources of product vulnerability information:

Android
CentOS
Cisco
Debian
F5 products
Fortinet
Microsoft
Oracle Linux
Red Hat
SUSE
Trend Micro
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk