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-iphone-rce-dos-U2PsSkz3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-dZROE8Lc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-sqlinj-HD1JeEAX
   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-sdwanvman-infodis1-YuQ5ScHB
   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-3aKhXwvS
   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/2021dsa-4864
   https://www.debian.org/security/2021dsa-4865
   https://www.debian.org/security/2021dsa-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!

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

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

13. SUSE


14. Trend Micro Products

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

15. Ubuntu

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

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