



Zero-day exploit of Exchange Server vulnerability

CRITICALITY



11/11/2021

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

Zero-day exploit of Exchange Server 2016 and 2019 vulnerability (CVE-2021-42321) that allows threat actors to execute code remotely on vulnerable servers. Microsoft has patched the vulnerability.



Threat Details

Microsoft urges administrators to instantly patch a high severity Exchange server vulnerability that may allow successfully authenticated threat actors to execute code remotely on vulnerable servers. Tracked as CVE-2021-42321 originates from an improper validation of cmdlet arguments, used in PowerShell environments. The vulnerability will be successfully exploited if the threat actor is successfully authenticated.

On- premises Microsoft Exchange servers 2016 and 2019 and Exchange Hybrid mode are vulnerable to CVE-2021-42321. Exchange online is not affected.

The NCSC recommends patching the servers immediately to protect your environment.

Also, Microsoft has added a new Exchange Server feature named Microsoft Exchange Emergency Mitigation (EM) that provides automated protection for vulnerable Exchange servers. The EM service runs as a Windows service on an Exchange Mailbox server. The September 2021 CU (or later) on Exchange Server 2016 or Exchange Server 2019, the EM service will be installed automatically on servers with the Mailbox role. The EM service will not be installed on Edge Transport servers. EM protect the server by automatically applying interim mitigations for high-risk security bugs to secure on-premises servers against incoming attacks and give admins additional time to apply security updates.

The use of the EM service is optional. The users can disable the feature if they do not want Microsoft to automatically apply mitigations to the Exchange servers.

Recommendations



 <u>Prevention</u> • Appendix A contains the recommendations to prevent such attacks.	 <u>Detection</u> • Appendix B contains a sample of Indicators of compromise of this threat the full list is in the attached file.
---	--

References

CVE-2021- 42321: Microsoft Exchange Server Remote Code Execution Vulnerability.(2021). Retrieved from Microsoft, MSRC: <https://m. src.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321>

Released: November 2021 Exchange Server Security Updates. (2021). Retrieved from Microsoft: <https:// techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2021-exchange-server-security-updates/ba-p/2933169>

Microsoft urges Exchange admins to patch bug exploited in the wild. (2021). Retrieved from BleepingComputer: <https://www.bleepingcomputer.com/news/microsoft/microsoft-urges-exchange-admins-to-patch-bug-exploited-in-the-wild/amp/>



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all entities to update the affected Exchange Server versions immediately to the latest version. Microsoft are providing two update paths, as shown in the figure below:



Microsoft Exchange Server update paths

NCSC recommends enabling Microsoft Exchange Emergency Mitigation (EM) feature in the exchange server.



Appendix B – Detection

To check if any of your Exchange servers were hit by CVE-2021-42321 exploitation attempts, please run the following PowerShell query on each Exchange server to check for specific events in the Event Log:

```
Get-EventLog -LogName Application -Source "MSExchange Common" -EntryType  
Error | Where-Object { $_.Message -like "*BinaryFormatter.Deserialize*" }
```



Appendix C – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.