cfcunderwriting.com

Remediation Guidance: ProxyShell Vulnerabilities

> The below information is a guide compiled by CFC Response globally to assist organisations in detecting, eradicating and remediating the ProxyShell vulnerabilities in Microsoft Exchange Server.

Recommended Response Steps

1. **Deploy** July 2021 security updates for Microsoft Exchange.
2. **Investigate** for exploitation or indicators of persistence.
3. **Remediate** any identified exploitation or persistence and investigate your environment for indicators of lateral movement or further compromise.

Deploy Updates

Affected devices include:

- Exchange Server 2013 up to CU23
- Exchange Server 2016 up to CU20
- Exchange Server 2019 up to CU9

Exchange Online, AKA Office 365 or Microsoft 365, is **not** affected. Exchange Server 2010 is not affected, but reached end-of-life in October 2020, so we strongly recommend not to use Exchange Server 2010.

Microsoft recommends using their Exchange Server Health Checker script to get an inventory of server patch levels. This script is available here: https://microsoft.github.io/CSS-Exchange/Diagnostics/HealthChecker/

Updates are available here: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-july-2021-exchange-server-security-updates/ba-p/2523421

If for whatever reason you cannot immediately update your server, the recommended temporary mitigation strategy is to block incoming, external traffic over port 443 to Exchange servers.

Investigate

Successful exploitation can be detected through reverse proxy logs. Examine incoming web requests over port 443 against uri_path '/autodiscover/autodiscover.json', with a status code of 200, 301 or 302 containing the following strings:

powershell
mapi/nspi

mapi/emsmdb
/EWS","X-Rps-CAT

Attackers exploiting the vulnerability are then dropping web shells onto the compromised device. After this, they can issue additional commands such as downloading and executing malicious binaries (such as .exe files). Look for any unexpected or recently created .aspx files in the following directories and subdirectories on the affected device:

C:\inetpub\wwwroot\aspnet_client\system_web
C:\inetpub\wwwroot\aspnet_client
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ecp\auth
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current
C:\ProgramData
C:\Users\All Users

Possible web shell locations are being detected by Huntress, and examples of these locations are available on their website: https://www.huntress.com/blog/rapid-response-microsoft-exchange-servers-still-vulnerable-to-proxyshell-exploit.

Attackers are establishing persistence on compromised devices by creating scheduled tasks to periodically execute suspicious files. You should therefore review all scheduled tasks on a device by looking at the Task Scheduler, and investigating any tasks that were recently created or unexpected.

Remediate

If you should find .aspx files in any of these paths mentioned above, copy the suspicious files into a .zip archive and securely store the files elsewhere for future investigation.

Once any suspicious files are securely copied and scheduled tasks are investigated, turn on Microsoft Defender Antivirus to detect and remove web shells. Defender with real-time protection enabled is highly recommended.
If Defender is unavailable on your system you can alternatively run the Microsoft Safety Scanner (https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download) to detect and remove web shells. You should run the 32-bit or 64-bit version, depending on your server.

If Indicators of Compromise detect a web shell, you should change all Active Directory passwords, starting with administrator accounts.

Finally, if Indicators of Compromise are found, a full reset of the krbtgt account should be completed to invalidate any active Kerberos tickets. This must be done twice to ensure all existing tickets are fully invalidated. Further information about this is available here: https://docs.microsoft.com/en-

us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn745899(v=ws.11)?redirectedfrom=MSDN#krbtgt-account.

General Hardening

Please see below for some general suggestions on enhancing your organisation's security posture:

- Patch early and patch often so that attackers do not have the time to exploit a vulnerability before you have had the chance to patch it.
- Enforce the use of strong, unique passwords across your infrastructure and enforce an account lockout policy. This will prevent attackers guessing passwords or cracking hashes to gain unauthorised access.
- Ensure protection mechanisms, such as firewalls and an antivirus solution, are in place. A local firewall and a boundary firewall are recommended for an in-depth approach. Ensure your antivirus engine and definitions are kept up to date.
- Ensure multi-factor authentication is in place for all external access, such as Outlook Web Access.

References

https://msrc.microsoft.com/update-guide/deployments
https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell
https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/
https://davinsi.com/threat-advisory-how-to-respond-to-proxyshell-the-latest-exploit-against-exchange/