Remediation Guidance: ProxyLogon Vulnerability

> The below information is a guide compiled by CFC Response globally to assist organizations in detecting, eradicating and remediating the March 2021 vulnerability in Microsoft Exchange Server.

Recommended response steps

1. Deploy updates to affected Exchange Servers.
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.

Microsoft recommends that you update and investigate in parallel, but if you must prioritize one, prioritize updating and mitigation of the vulnerability.

Deploy updates

The high-level summary of Microsoft's guidance is:

- Exchange Online is not affected.

- Exchange 2003 and 2007 are no longer supported but are not believed to be affected by the March 2021 vulnerabilities. You must upgrade to a supported version of Exchange to ensure that you are able to secure your deployment against vulnerabilities fixed in current versions of Microsoft Exchange and future fixes for security issues.

- Exchange 2010 is only impacted by CVE-2021-26857, which is not the first step in the attack chain. Organizations should apply the update and then follow the guidance below to investigate for potential exploitation and persistence.

- Exchange 2013, 2016, and 2019 are impacted. Immediately deploy the updates and apply mitigations described below. For help identifying which updates you need to get, follow the guidance available here: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901. To help identify which CUs are needed for your deployment, you can use the linked Health Checker script available here: https://github.com/dpaulson45/HealthChecker#download.

Updates are available here: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

If for whatever reason you cannot immediately update your server, please see the temporary mitigation strategies suggested by Microsoft here: https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

Investigate

Scan the affected Microsoft Exchange Server's logs for Indicators of Compromise using Microsoft's tool available here: https://github.com/microsoft/CSS-Exchange/tree/main/Security https://github.com/microsoft/CSS-Exchange/tree/main/Security.

Remediate

If Indicators of Compromise are detected by Microsoft's tool, such as web shells, copy the suspicious files into a .zip archive and securely store the files elsewhere for future investigation.

Once any suspicious files are securely copied, 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 organization'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-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

https://github.com/microsoft/CSS-Exchange/tree/main/Security

https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708