==========

Alert on Zero-day Vulnerabilities in Microsoft Exchange Server

Microsoft has officially disclosed that they are investigating two zero-day security vulnerabilities impacting Exchange Server 2013, 2016, and 2019 following reports of in-the-wild exploitation.

The vulnerability:

1. **CVE-2022-41040**, is a Server-Side Request Forgery (SSRF) vulnerability.
2. **CVE-2022-41082**, allows remote code execution (RCE) when PowerShell is accessible to the attacker.

In these attacks, CVE-2022-41040 can enable an authenticated attacker to remotely trigger CVE-2022-41082. It should be noted that authenticated access to the vulnerable Exchange Server is necessary to successfully exploit either vulnerability. Microsoft is working on an accelerated timeline to release a fix. Until then, the following mitigation steps need to be followed to protect themselves from these attacks.

The attacker installs Chopper web shell by exploiting the above vulnerability. It is suspected that state sponsored actors are behind these attacks.

Mitigations:

Exchange Online customers do not need to take any action.(Hybrid deployment could also be vulnerable)

On-premises Microsoft Exchange customers are advised to add a blocking rule in IIS Manager as a temporary workaround to mitigate potential threats.

To reduce the risk of exploitation, Customers can follow the below instructions.

1. Open IIS Manager.
2. Select Default Web Site.
3. In the Feature View, click URL Rewrite.
4. In the Actions pane on the right-hand side, click Add Rule(s)…
5. Select Request Blocking and click OK.
6. Add the string ".*autodiscover\.json.*\@.*Powershell.*" (excluding quotes).
7. Select "Regular Expression" under Using.
8. Select Abort Request under How to block and then click OK.

9. Expand the rule and select the rule with the pattern .*autodiscover\.json.*\@.*Powershell.* and click Edit under Conditions.
10. Change the Condition input from {URL} to {REQUEST_URI}

It is strongly recommending "**to disable remote PowerShell access for non-admin users"** to Exchange Server customers as a precautionary measure.

Threat Intelligence & Malware Group
Kerala Police Cyberdome

References:
https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/

https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/