Hotfix for Exchange Zero Day Vulnerabilities

Summary

This article provides information about Exchange Zero day Vulnerabilities and how to fix these while using MachPanel.

Applies To

This article applies to Exchange 2013, 2016, 2019

Security Alert:

Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server – Microsoft Security Response Center

Investigate if you are affected: Get-ChildItem -Recurse -Path C:\inetpub\logs\LogFiles -Filter "*.log" | Select-String -Pattern 'powershell.*autodiscover\.json.*\@.*200'

Mitigations:

- URL Rewrite rule
- Disable remote PowerShell access for non-admins

URL Rewrite rule:

- Option 1: For customers who have the Exchange Emergency Mitigation Service (EEMS) enabled, Microsoft released the URL Rewrite mitigation for Exchange Server 2016 and Exchange Server 2019. The mitigation is enabled automatically and is updated to include the URL Rewrite rule improvements
- Option 2: Microsoft created the EOMTv2 script for the URL Rewrite mitigation steps and updated it to include the URL Rewrite rule improvements. EOMTv2 script will auto-update on Internet connected machines and the updated version will show as 22.10.05.2304. The script should be re-run on any Exchange Server without EEMS enabled.
- Option 3: Customers can follow the instructions as stated at Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server – Microsoft Security

Hotfix for Exchange Zero Day Vulnerabilities

Response Center

Disable remote PowerShell access for non-admins:

Please refer to Control remote PowerShell access to Exchange servers | Microsoft Learn to disable remote PowerShell access for users per user and bulk users.

How MachPanel cares about its customers?

Deploy Hotfix v7.0.41 HF2

- Afterwards Every new created Mailbox will come up with RemotePowerShellEnabled as $false.
- For Existing Mailboxes, please trigger Fix security permissions per tenant.

Caution: MachPanel Service / Provisioning account should be kept as RemotePowerShellEnabled as $true.

MachPanel Knowledgebase
https://kb.machsol.com/Knowledgebase/55717/Hotfix-for-Exchange-Zero-Day-Vul...