

 FLASH

Microsoft Exchange Zero-Day Vulnerabilities

ZEROFOX INTELLIGENCE

F-2022-09-30a

Classification: TLP: CLEAR

Criticality: MEDIUM

Intelligence Requirements: Vulnerability

September 30, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:00 AM (EDT) on September 30, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Microsoft Exchange Zero-Day Vulnerabilities

Key Findings

- Two zero-day vulnerabilities were identified that affect Microsoft Exchange Server versions 2013, 2016, and 2019. On-premises Exchange customers are impacted, and possibly those operating hybrid server environments as well.
- Active exploitation in the wild has been identified.
- Workarounds are available, and Microsoft encourages users to enact URL rewrite instructions and block exposed Remote PowerShell ports.

Analyst Commentary

On September 29, 2022, Microsoft confirmed two zero-day vulnerabilities—tracked as CVE-2022-41040 and CVE-2022-41082—affecting its Exchange Server, versions 2013, 2016, and 2019.¹ Multiple sources disclosed the vulnerabilities, and state that the vulnerabilities are being actively exploited in the wild.²³ While Microsoft has advised that only on-premises Exchange customers are impacted and that customers with Exchange Online do not need to take any action, customers that operate a hybrid server could be impacted.

CVE-2022-41040 is a Server-Side Request Forgery (SSRF) vulnerability that can enable an authenticated attacker to remotely trigger CVE-2022-41082, a remote code

¹

[hXXps://msrc-blog.microsoft\[.\]com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/](https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/)

²

[hXXps://www.gteltsc\[.\]vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html](https://www.gteltsc[.]vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html)

³ [hXXps://twitter\[.\]com/GossiTheDog/status/1575762721353916417](https://twitter[.]com/GossiTheDog/status/1575762721353916417)



execution (RCE) vulnerability that can be executed by threat actors that have access to PowerShell. From there, threat actors can establish persistence, exfiltrate data, or move laterally across compromised networks. Microsoft states that threat actors must have authenticated access to exploit either vulnerability.

The exploit chain follows a similar path to the April 2021 Microsoft Exchange ProxyShell vulnerabilities, indicating the possibility that patches deployed in 2021 did not fully fix the issues.

Recommendations

Microsoft shared instructions for an official workaround through the Microsoft Security Response Center (MSRC) website on September 29, 2022. There is no patch currently available. Microsoft encourages users to review and enact URL rewrite instructions and block exposed Remote PowerShell ports (HTTP: 5985 and HTTPS: 5986). Rewrite instructions are as follows:

1. Open the IIS Manager.
2. Expand the Default Web Site.
3. Select Autodiscover.
4. In the Feature View, click URL Rewrite.
5. In the Actions pane on the right-hand side, click Add Rules.
6. Select Request Blocking and click OK.
7. Add String `"*.autodiscover\.json.*\@.*Powershell.*"` (excluding quotes) and click OK.
8. Expand the rule and select the rule with the Pattern `"*.autodiscover\.json.*\@.*Powershell.*"` and click Edit under Conditions.
9. Change the condition input from {URL} to {REQUEST_URI}

It is advised that admins scan their network for indicators of compromise by running the following PowerShell command:⁴

- `Get-ChildItem -Recurse -Path <Path_IIS_Logs> -Filter "*.log" | Select-String -Pattern 'powershell.*autodiscover\.json.*\@.*200'`

4

[hXXps://www.gteltsc\[.\]vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html](https://www.gteltsc[.]vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html)



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	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.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	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.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.