Microsoft

Light ☀

Microsoft Security ⌄

🏠 **Blog home** / Threat intelligence

Search the blog
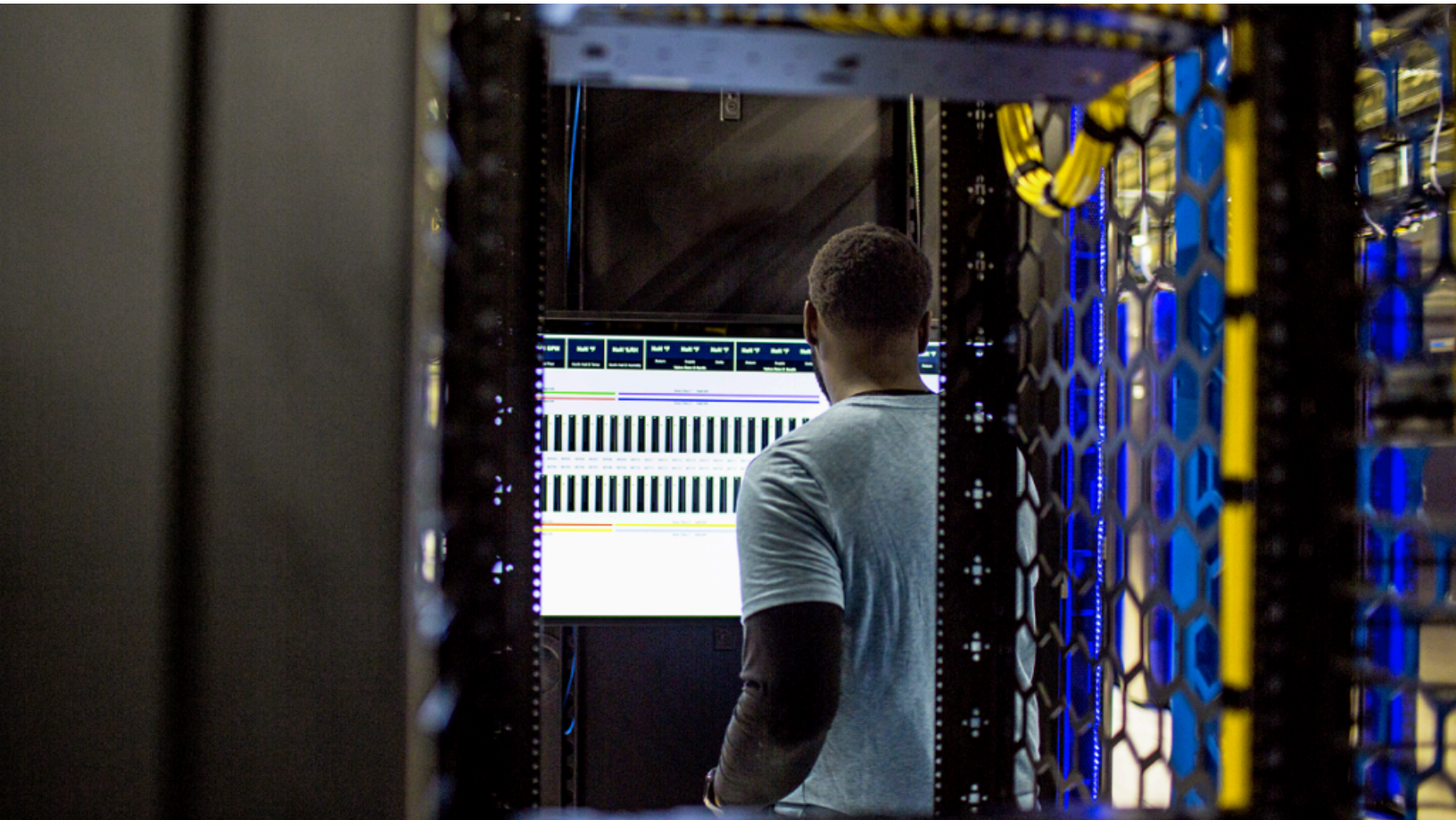
Research **Threat intelligence** **Threat actors**

7 min read

Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082

By Microsoft Threat Intelligence

September 30, 2022

Vulnerabilities and exploits   MITRE ATT&CK

November 8, 2022 update – Microsoft has released patches for these issues. While Microsoft has not seen any further exploitation of these vulnerabilities in the wild since the targeted use in August, it is highly recommended that organizations patch their systems as attackers often reverse engineer patches to develop exploits.

October 1, 2022 update – Added information about *Exploit:Script/ExchgProxyRequest.A*, Microsoft Defender AV's robust detection for exploit behavior related to this threat. We also removed a section on MFA as a mitigation, which was included in a prior version of this blog as standard guidance.

Microsoft is aware of limited targeted attacks using two reported zero-day vulnerabilities affecting Microsoft Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019. The first one, identified as CVE-2022-41040, is a server-side request forgery (SSRF) vulnerability, while the second one, identified as CVE-2022-41082, allows remote code execution (RCE) when Exchange PowerShell is accessible to the attacker. Refer to the Microsoft Security Response Center blog for mitigation guidance regarding these vulnerabilities.

CVE-2022-41040 can enable an authenticated attacker to remotely trigger CVE-2022-41082. However, authenticated access to the vulnerable Exchange Server is necessary to successfully exploit either vulnerability, and they can be used separately.

Microsoft released patches for these issues on November 8, 2022. Customers who haven't patched yet are urged to do so as soon as possible. Mitigation guidance is still provided here for organizations that have not yet deployed a mitigation, and can be used while deploying patches. Customers are encouraged to enable the Exchange Emergency Mitigation Service, which allows mitigations to be deployed automatically for future incidents.

Microsoft Defender Antivirus and Microsoft Defender for Endpoint detect malware and activity associated with these attacks. Microsoft will continue to monitor threats that take advantage of these vulnerabilities and take necessary response actions to protect customers.

Analysis of observed activity

Attacks using Exchange vulnerabilities prior to public disclosure

MSTIC observed activity related to a single activity group in August 2022 that achieved initial access and compromised Exchange servers by chaining CVE-2022-41040 and CVE-2022-41082 in a small number of targeted attacks. These attacks

installed the Chopper web shell to facilitate hands-on-keyboard access, which the attackers used to perform Active Directory reconnaissance and data exfiltration. Microsoft observed these attacks in fewer than 10 organizations globally. MSTIC assesses with medium confidence that the single activity group is likely to be a state-sponsored organization.

Microsoft researchers were investigating these attacks to determine if there was a new exploitation vector in Exchange involved when the Zero Day Initiative (ZDI) disclosed CVE-2022-41040 and CVE-2022-41082 to Microsoft Security Response Center (MSRC) in September 2022.
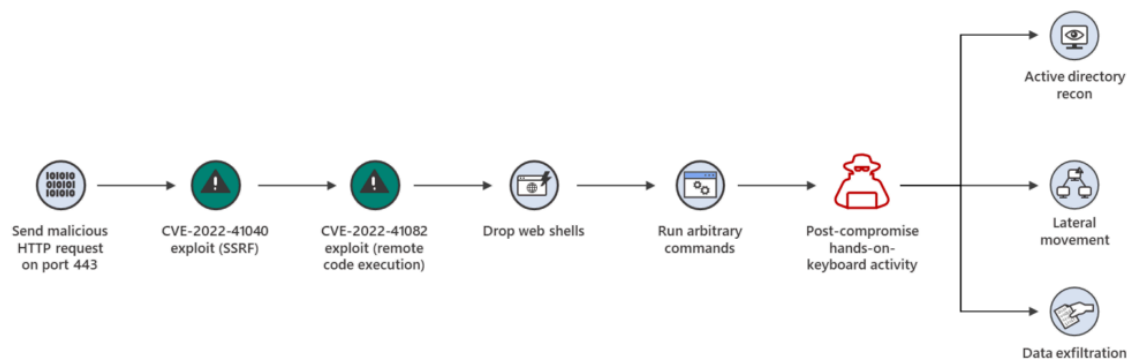

Figure 1: Diagram of attacks using Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082

Observed activity after public disclosure

On September 28, 2022, GTSC released a blog disclosing an exploit previously reported to Microsoft via the Zero Day Initiative and detailing its use in an attack in the wild. Their blog details one example of chained exploitation of CVE-2022-41040 and CVE-2022-41082 and discusses the exploitation details of CVE-2022-41040. It is expected that similar threats and overall exploitation of these vulnerabilities will increase, as security researchers and cybercriminals adopt the published research into their toolkits and proof of concept code becomes available.

While these vulnerabilities require authentication, the authentication needed for exploitation can be that of a standard user. Standard user credentials can be acquired

via many different attacks, such as password spray or purchase via the cybercriminal economy. Prior Exchange vulnerabilities that require authentication have been adopted into the toolkits of attackers who deploy ransomware, and these vulnerabilities are likely to be included in similar attacks due to the highly privileged access Exchange systems confer onto an attacker.

Mitigation

Customers should refer to Microsoft Security Response Center's post for the latest on mitigations for the Exchange product.

Microsoft Exchange Server customers using Microsoft 365 Defender are advised to follow this checklist:

- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Turn on tamper protection features to prevent attackers from stopping security services.
- Run EDR in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Enable network protection to prevent applications or users from accessing malicious domains and other malicious content on the internet.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Use device discovery to increase your visibility into your network by finding unmanaged devices on your network and onboarding them to Microsoft Defender for Endpoint.

Detection

Microsoft Defender Antivirus

Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082 | Microsoft Security Blog - 31/10/2024 16:15 https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/

Microsoft Exchange AMSI integration and Antivirus Exclusions

Exchange supports the integration with the Antimalware Scan Interface (AMSI) since the June 2021 Quarterly Updates for Exchange. It is highly recommended to ensure these updates are installed and AMSI is working using the [guidance provided by the Exchange Team](#), as this integration provides the best ability for Defender Antivirus to detect and block exploitation of vulnerabilities on Exchange.

Many organizations exclude Exchange directories from antivirus scans for performance reasons. It's highly recommended to audit AV exclusions on Exchange systems and assess if they can be removed without impacting performance and still ensure the highest level of protection. Exclusions can be managed via Group Policy, PowerShell, or systems management tools like System Center Configuration Manager.

To audit AV exclusions on an Exchange Server running Defender Antivirus, launch the *Get-MpPreference* command from an elevated PowerShell prompt.

If exclusions cannot be removed for Exchange processes and folders, running Quick Scan in Defender Antivirus scans Exchange directories and files regardless of exclusions.

Microsoft Defender Antivirus detects the post-exploitation malware currently used in-the-wild exploitation of this vulnerability as the following:

Microsoft Defender Antivirus detections	MITRE ATT&CK Tactics observed
[Exploit:Script/ExchgProxyRequest.A](#) [Exploit:Script/ExchgProxyRequest.B](#) [Exploit:Script/ExchgProxyRequest.C](#) (the most robust defense from Microsoft Defender AV against this threat; requires Exchange AMSI to be enabled)	Initial Access
[Backdoor:ASP/Webshell.Y](#)	Persistence
[Backdoor:Win32/RewriteHttp.A](#)	Persistence

Backdoor:JS/SimChocexShell.A!dha	Persistence
Behavior:Win32/IISExchgDropWebshell.A!dha	Persistence
Behavior:Win32/IISExchgDropWebshell.A	Persistence
Trojan:Win32/IISExchgSpawnCMD.A	Execution
Trojan:Win32/WebShellTerminal.A	Execution
Trojan:Win32/WebShellTerminal.B	Execution

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint detects post-exploitation activity. The following alerts could be related to this threat:

Indicators of attack	MITRE ATT&CK Tactics observed
Possible web shell installation	Persistence
Possible IIS web shell	Persistence
Suspicious Exchange Process Execution	Execution
Possible exploitation of Exchange Server vulnerabilities (Requires Exchange AMSI to be enabled)	Initial Access
Suspicious processes indicative of a web shell	Persistence
Possible IIS compromise	Initial Access

As of this writing, Defender for Endpoint customers with Microsoft Defender Antivirus enabled can also detect the web shell malware used in in-the-wild exploitation of this vulnerability with the following alerts:

Indicators of attack	MITRE ATT&CK Tactics observed
'Chopper' malware was detected on an IIS Web server	Persistence
'Chopper' high-severity malware was detected	Persistence

Microsoft Defender Threat Intelligence

Microsoft Defender Threat Intelligence (MDTI) maps the internet to expose threat actors and their infrastructure. As indicators of compromise (IOCs) associated with threat actors targeting the vulnerabilities described in this writeup are surfaced, Microsoft Defender Threat Intelligence Community members and customers can find summary and enrichment information for all IOCs within the Microsoft Defender Threat Intelligence portal.

Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management identifies devices in an associated tenant environment that might be affected by CVE-2022-41040 and CVE-2022-41082. These vulnerabilities have been added to the CISA known exploited vulnerabilities list and are considered in the overall organizational exposure score. Customers can use the following capabilities to identify vulnerable devices and assess exposure:

- Use the dedicated dashboard for each of CVE-2022-41040 and CVE-2022-41082 to get a consolidated view of various findings across vulnerable devices and software.
- Use the *DeviceTvmSoftwareVulnerabilities* table in advanced hunting to identify vulnerabilities in installed software on devices. Refer to the following query to run:

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2022-41040", "CVE-2022-41082")
```

Figure 2: Screenshot of the CVE information page where users can also take a look at related exposed device, software information, open vulnerability page, report inaccuracy, or read other useful references.

NOTE: The assessments above do not currently account for the existence of a workaround mitigation on the device. Microsoft will continue to improve these capabilities based on the latest information from the threat landscape.

Advanced hunting

Microsoft Sentinel

Based on what we're seeing in the wild, Microsoft Sentinel customers can use the following techniques for web shell-related attacks connected to these vulnerabilities. Our post on web shell threat hunting with Microsoft Sentinel also provides guidance on looking for web shells in general.

The Exchange SSRF Autodiscover ProxyShell detection, which was created in response to ProxyShell, can be used for queries due to functional similarities with this threat. Also, the new Exchange Server Suspicious File Downloads and Exchange Worker Process Making Remote Call queries specifically look for suspicious downloads or activity in IIS logs. In addition to these, we have a few more that could be helpful in looking for post-exploitation activity:

- Exchange OAB virtual directory attribute containing potential web shell
- Web shell activity
- Malicious web application requests linked with Microsoft Defender for Endpoint alerts
- Exchange IIS worker dropping web shell
- Web shell detection

Microsoft 365 Defender

To locate related activity, Microsoft 365 Defender customers can run the following advanced hunting queries:

Chopper web shell

Use this query to hunt for Chopper web shell activity:

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "w3wp.exe"
| where ProcessCommandLine has_any ("&ipconfig&echo", "&quser&echo",
"&whoami&echo", "&c:&echo", "&cd&echo", "&dir&echo", "&echo [E]",
"&echo [S]")
```

Suspicious files in Exchange directories

Use this query to hunt for suspicious files in Exchange directories:

```
DeviceFileEvents
| where Timestamp >= ago(7d)
| where InitiatingProcessFileName == "w3wp.exe"
| where FolderPath has "FrontEnd\\HttpProxy\\"
| where InitiatingProcessCommandLine contains "MSExchange"
| project FileName,FolderPath,SHA256, InitiatingProcessCommandLine,
DeviceId, Timestamp
```

External attack surface management

Microsoft Defender External Attack Surface Management

[Microsoft Defender External Attack Surface Management](#) continuously discovers and maps your digital attack surface to provide an external view of your online infrastructure. Attack Surface Insights are generated by leveraging vulnerability and infrastructure data to showcase the key areas of concern for your organization.

A High Severity Observation has been published to surface assets within an attack surface which should be examined for application of the mitigation steps described above. This insight, titled *CVE-2022-41082 & CVE-2022-41040 – Microsoft Exchange Server Authenticated SSRF and PowerShell RCE,* can be found under the high severity observations section of the Attack Surface Summary dashboard.

Related Posts

Research Threat intelligence

Microsoft Copilot for Security Threat actors

Feb 14 · 13 min read

Staying ahead of threat actors in the age of AI >

Microsoft, in collaboration with OpenAI, is publishing research on emerging threats in the age of AI, focusing on identified activity associated with known threat actors Forest Blizzard, Emerald Sleet, Crimson Sandstorm, and others. The observed activity includes prompt-injections, attempted misuse of large language models (LLM), and fraud.

Research Threat intelligence

Influence operations

Mar 2, 2023 · 10 min read

New research, tooling, and partnerships for more secure AI and machine learning >

At Microsoft, we've been working on the challenges and opportunities of AI for years. Today we're sharing some recent developments so that the community can be better informed and better equipped for a new world of AI exploration.

Research Threat intelligence

Microsoft Defender

Attacker techniques, tools, and infrastructure

Dec 6, 2022 · 18 min read

DEV-0139 launches targeted attacks against the cryptocurrency industry >

Microsoft security researchers investigate an attack where the threat actor, tracked DEV-0139, used chat groups to target specific

News Analyst reports

Microsoft Security Experts

Nov 9, 2022 · 4 min read

Microsoft Defender Experts for Hunting demonstrates industry-leading protection in the 2022 MITRE Engenuity ATT&CK® Evaluations for Managed Services >

Microsoft Defender Experts for Hunting, our newest managed threat hunting service, delivered top-class results during the inaugural

cryptocurrency investment companies and run a backdoor within their network.

MITRE Engenuity ATT&CK® Evaluations for Managed Services. Defender Experts for Hunting provided a seamless, comprehensive, and rapid response to the simulated attack using expert-led threat hunting and an industry-leading platform—Microsoft 365 Defender.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Pro

Microsoft Store

Account profile

Education

Microsoft in education

Surface Laptop

Surface Laptop Studio 2

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices