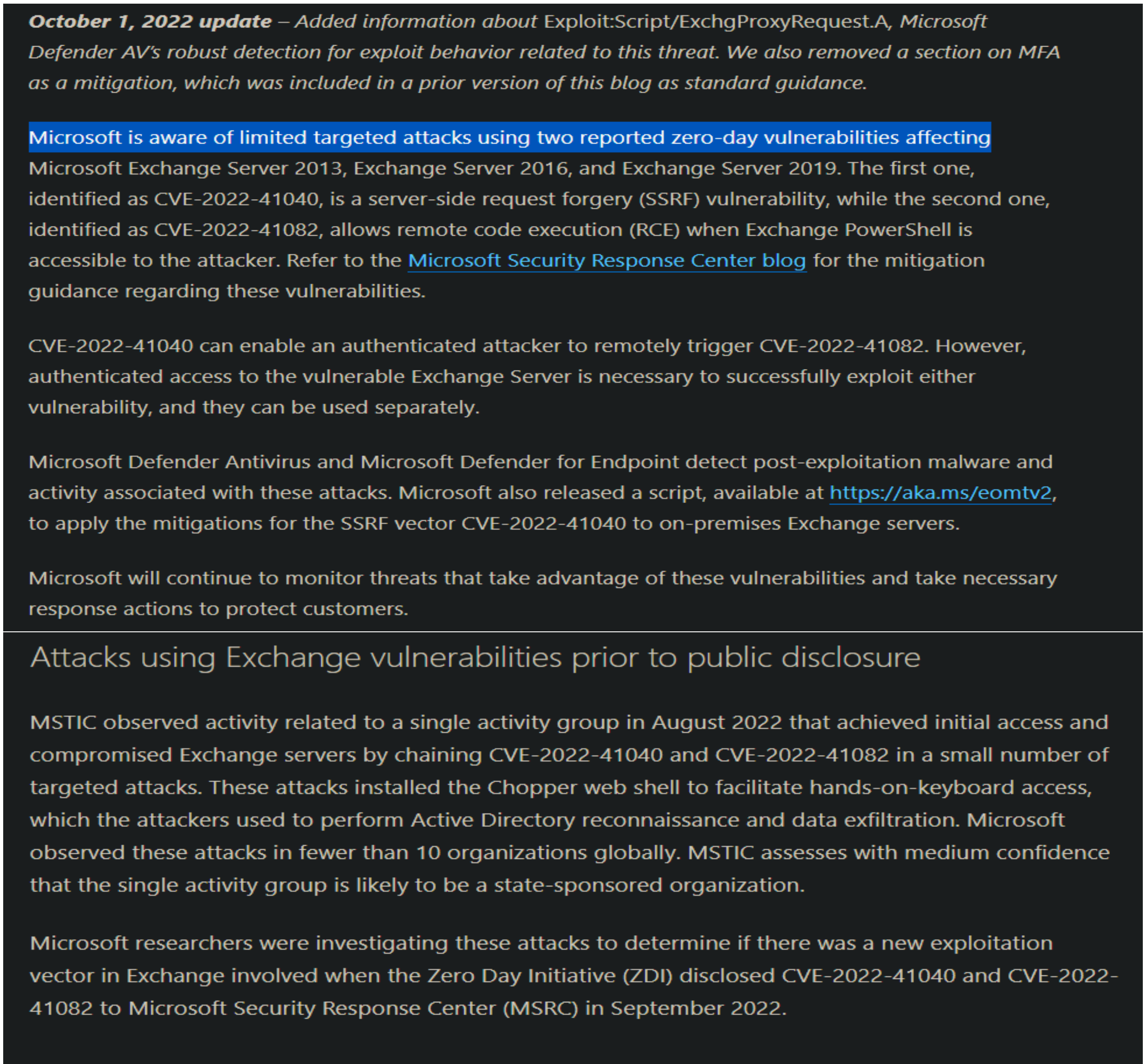
Exchange 2019 Vulnerabilities – CVE2022-41040 & 41082

Microsoft released info about Exchange vulnerabilities pertaining to targeted attack using zero day vulnerabilities. To fix exchange servers we should run PowerShell script that was released to fix this issue. Details are below with respective links.

https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/
https://microsoft.github.io/CSS-Exchange/Security/EOMTv2/



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 the 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.

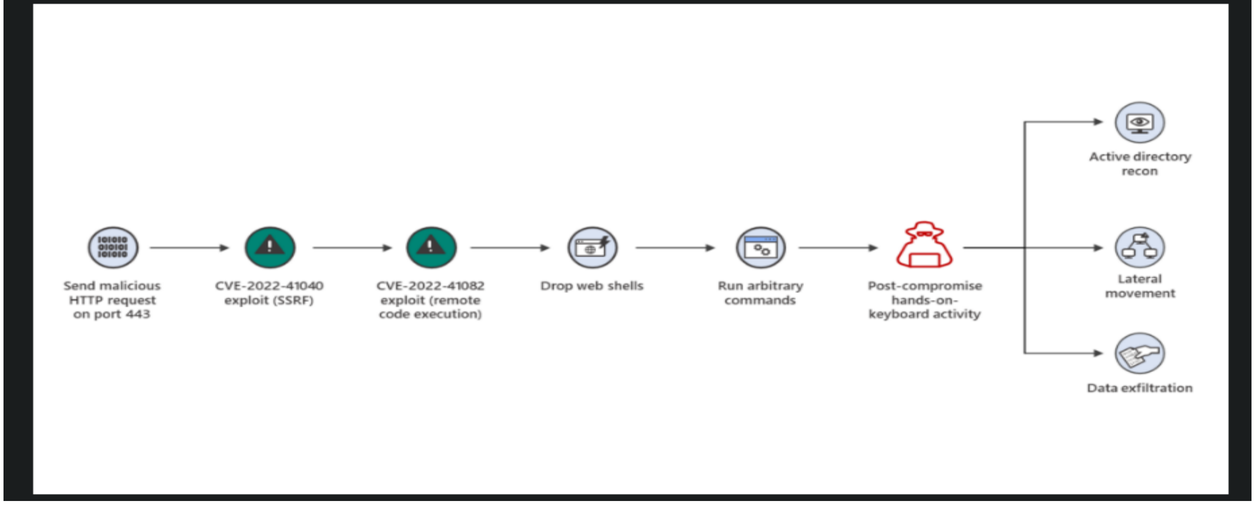
Microsoft Defender Antivirus and Microsoft Defender for Endpoint detect post-exploitation malware and activity associated with these attacks. Microsoft also released a script, available at https://aka.ms/eomtv2, to apply the mitigations for the SSRF vector CVE-2022-41040 to on-premises Exchange servers.

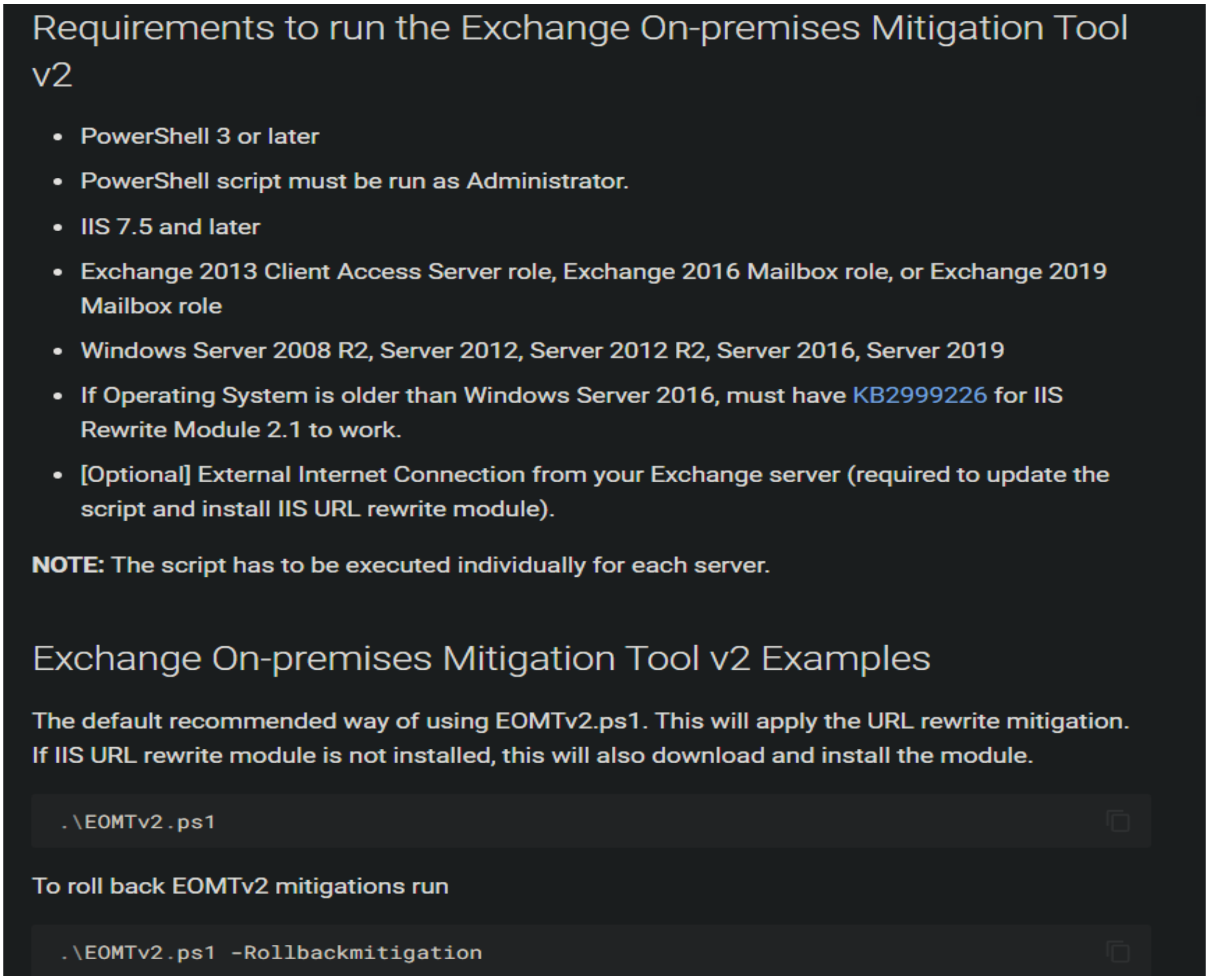
Microsoft will continue to monitor threats that take advantage of these vulnerabilities and take necessary response actions to protect customers.

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.


Send malicious HTTP request on port 443
CVE-2022-41040 exploit (SSRF)
CVE-2022-41082 exploit (remote code execution)
Drop web shells
Run arbitrary commands
Post-compromise hands-on-keyboard activity
Active directory recon
Lateral movement
Data exfiltration



Requirements to run the Exchange On-premises Mitigation Tool v2

- PowerShell 3 or later
- PowerShell script must be run as Administrator.
- IIS 7.5 and later
- Exchange 2013 Client Access Server role, Exchange 2016 Mailbox role, or Exchange 2019 Mailbox role
- Windows Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019
- If Operating System is older than Windows Server 2016, must have KB2999226 for IIS Rewrite Module 2.1 to work.
- [Optional] External Internet Connection from your Exchange server (required to update the script and install IIS URL rewrite module).

NOTE: The script has to be executed individually for each server.

Exchange On-premises Mitigation Tool v2 Examples

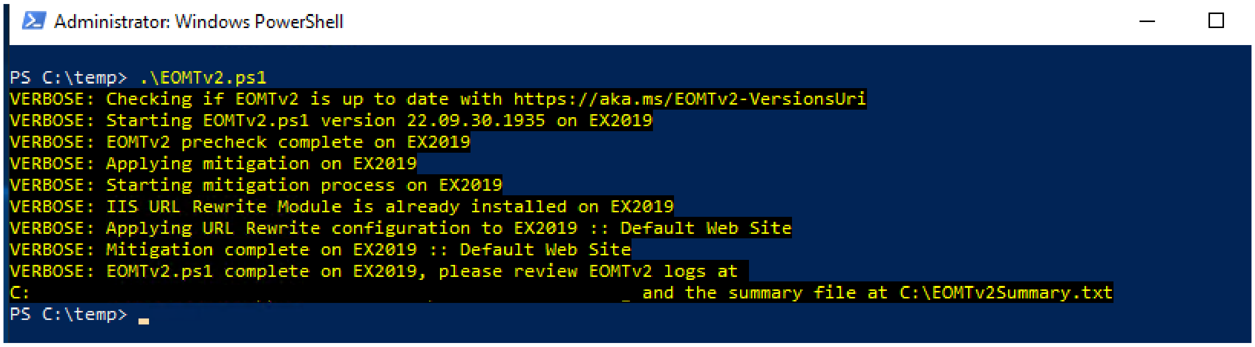
The default recommended way of using EOMTv2.ps1. This will apply the URL rewrite mitigation. If IIS URL rewrite module is not installed, this will also download and install the module.

```
.\EOMTv2.ps1
```

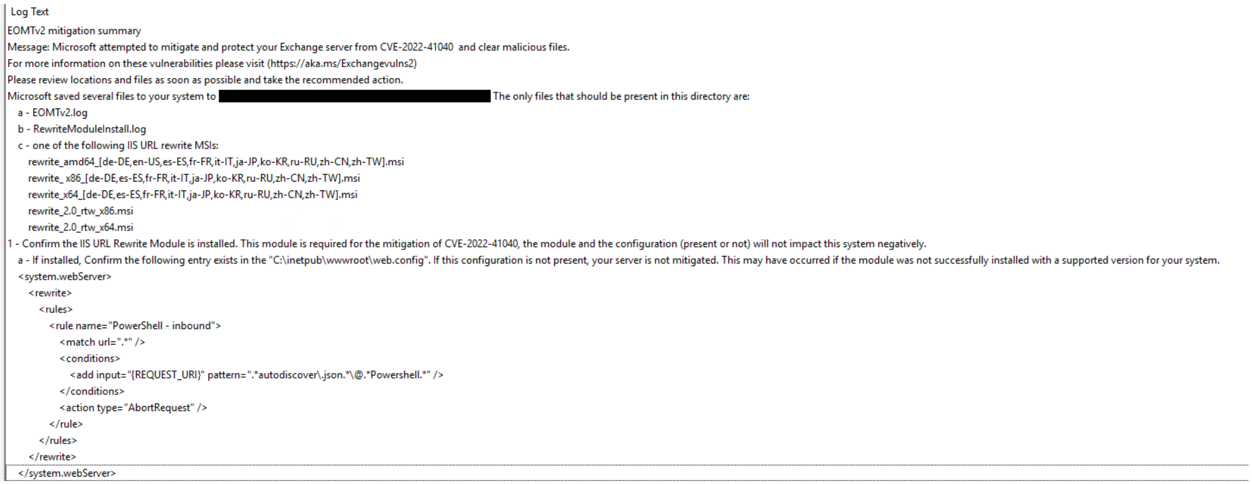
To roll back EOMTv2 mitigations run

```
.\EOMTv2.ps1 -Rollbackmitigation
```

Open PowerShell as Administrator and run the script.

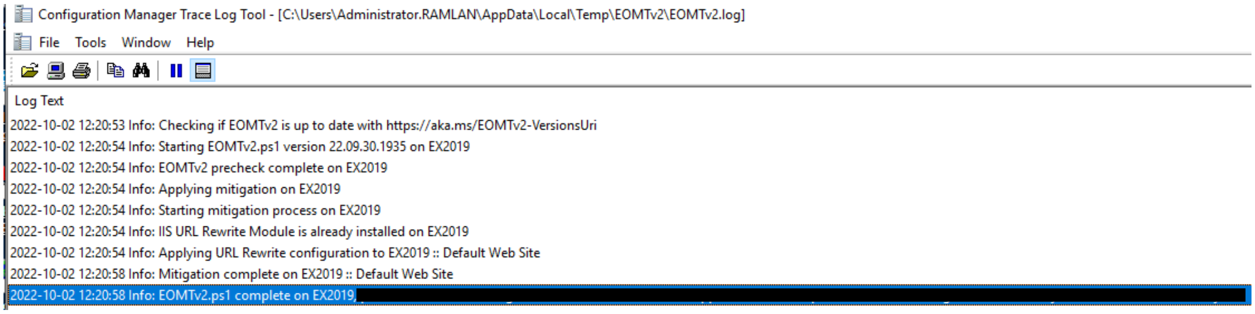


```
PS C:\temp> .\EOMTv2.ps1
VERBOSE: Checking if EOMTv2 is up to date with https://aka.ms/EOMTv2-VersionsUri
VERBOSE: Starting EOMTv2.ps1 version 22.09.30.1935 on EX2019
VERBOSE: EOMTv2 precheck complete on EX2019
VERBOSE: Applying mitigation on EX2019
VERBOSE: Starting mitigation process on EX2019
VERBOSE: IIS URL Rewrite Module is already installed on EX2019
VERBOSE: Applying URL Rewrite configuration to EX2019 :: Default Web Site
VERBOSE: Mitigation complete on EX2019 :: Default Web Site
VERBOSE: EOMTv2.ps1 complete on EX2019, please review EOMTv2 logs at
C: [redacted] and the summary file at C:\EOMTv2Summary.txt
PS C:\temp> _
```



```
Log Text
EOMTv2 mitigation summary
Message: Microsoft attempted to mitigate and protect your Exchange server from CVE-2022-41040  and clear malicious files.
For more information on these vulnerabilities please visit (https://aka.ms/Exchangevulns2)
Please review locations and files as soon as possible and take the recommended action.
Microsoft saved several files to your system to [redacted] The only files that should be present in this directory are:
  a - EOMTv2.log
  b - RewriteModuleInstall.log
  c - one of the following IIS URL rewrite MSIs:
    rewrite_amd64_[de-DE,en-US,es-ES,fr-FR,it-IT,ja-JP,ko-KR,ru-RU,zh-CN,zh-TW].msi
    rewrite_ x86_[de-DE,es-ES,fr-FR,it-IT,ja-JP,ko-KR,ru-RU,zh-CN,zh-TW].msi
    rewrite_x64_[de-DE,es-ES,fr-FR,it-IT,ja-JP,ko-KR,ru-RU,zh-CN,zh-TW].msi
    rewrite_2.0_rtw_x86.msi
    rewrite_2.0_rtw_x64.msi
1 - Confirm the IIS URL Rewrite Module is installed. This module is required for the mitigation of CVE-2022-41040, the module and the configuration (present or not) will not impact this system negatively.
  a - If installed, Confirm the following entry exists in the "C:\inetpub\wwwroot\web.config". If this configuration is not present, your server is not mitigated. This may have occurred if the module was not successfully installed with a supported version for your system.
  <system.webServer>
    <rewrite>
      <rules>
        <rule name="PowerShell - inbound">
          <match url=".*" />
          <conditions>
            <add input="{REQUEST_URI}" pattern=".*autodiscover\.json.*\@.*Powershell.*" />
          </conditions>
          <action type="AbortRequest" />
        </rule>
      </rules>
    </rewrite>
  </system.webServer>
```

```
   <system.webServer>
       <rewrite>
           <rules>
               <rule name="EEMS M1.1 PowerShell - inbound" stopProcessing="true">
                   <match url=".*" />
                   <conditions>
                       <add input="{REQUEST_URI}" pattern=".*autodiscover\.json.*\@.*Powershell.*" />
                   </conditions>
                   <action type="AbortRequest" />
               </rule>
               <rule name="PowerShell - inbound">
                   <match url=".*" />
                   <conditions>
                       <add input="{REQUEST_URI}" pattern=".*autodiscover\.json.*\@.*Powershell.*" />
                   </conditions>
                   <action type="AbortRequest" />
               </rule>
           </rules>
       </rewrite>
   </system.webServer>
/configuration>
```



Configuration Manager Trace Log Tool - [C:\Users\Administrator.RAMLAN\AppData\Local\Temp\EOMTv2\EOMTv2.log]

```
2022-10-02 12:20:53 Info: Checking if EOMTv2 is up to date with https://aka.ms/EOMTv2-VersionsUri
2022-10-02 12:20:54 Info: Starting EOMTv2.ps1 version 22.09.30.1935 on EX2019
2022-10-02 12:20:54 Info: EOMTv2 precheck complete on EX2019
2022-10-02 12:20:54 Info: Applying mitigation on EX2019
2022-10-02 12:20:54 Info: Starting mitigation process on EX2019
2022-10-02 12:20:54 Info: IIS URL Rewrite Module is already installed on EX2019
2022-10-02 12:20:54 Info: Applying URL Rewrite configuration to EX2019 :: Default Web Site
2022-10-02 12:20:58 Info: Mitigation complete on EX2019 :: Default Web Site
2022-10-02 12:20:58 Info: EOMTv2.ps1 complete on EX2019, [redacted]
```

This concludes on how to fix above exchange vulnerabilities.

Thanks

Ram
2nd Oct 2022