ProxyNoShell: A Change in Tactics Exploiting ProxyShell Vulnerabilities

Breadcrumb

Blog

Joshua Goddard

Nov 17, 2021

5 mins read

Vulnerabilities

Threat Research

TTPs

In September 2021, Mandiant published a blog post from the Mandiant Managed Defense team about widespread exploitation of three vulnerabilities in on-premises Microsoft Exchange Servers which were collectively referred to as ProxyShell. Despite disclosure occurring in April 2021 and patches being released in April and May 2021, Mandiant's Incident Response team has continued to respond to compromises originating from exploitation of these vulnerabilities as recently as November 2021 and estimates that up to 30,000 internet-facing vulnerable servers still exist.

- CVE-2021-34473 - Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-34523 - Microsoft Exchange Server Elevation of Privilege Vulnerability
- CVE-2021-31207 - Microsoft Exchange Server Security Feature Bypass Vulnerability

In several recent Incident Response engagements, Mandiant has observed threat actors exploiting the vulnerabilities in different ways than previously reported. Most notably, the writing of web shells via export of exchange certificate requests instead of mailbox exports, and exploitation of the first two vulnerabilities in the exploit chain only to achieve remote PowerShell and create new mailboxes, assign them privileged access to other mailboxes, then access them via Outlook Web Access (OWA). Mandiant is reporting these changes in tactics since the detection and response guidance previously issued focused exclusively on web shells originating from mailbox export.

Attack Paths with ProxyShell Vulnerabilities

Upon successful exploitation of the second stage of the ProxyShell vulnerability chain, a threat actor can execute any Microsoft Exchange PowerShell cmdlet via remote PowerShell within the context of a target user where remote PowerShell is enabled, most notably those with administrative permissions. Remote PowerShell is enabled for users by default in Microsoft Exchange.

At this second stage of exploitation, Mandiant has observed threat actors taking one of three attack paths leading to either a web shell or access to mailboxes, although any of the available Exchange PowerShell cmdlet's may be executed, providing threat actors with full Exchange administrative capabilities. Figure 1 provides an overview of these paths.

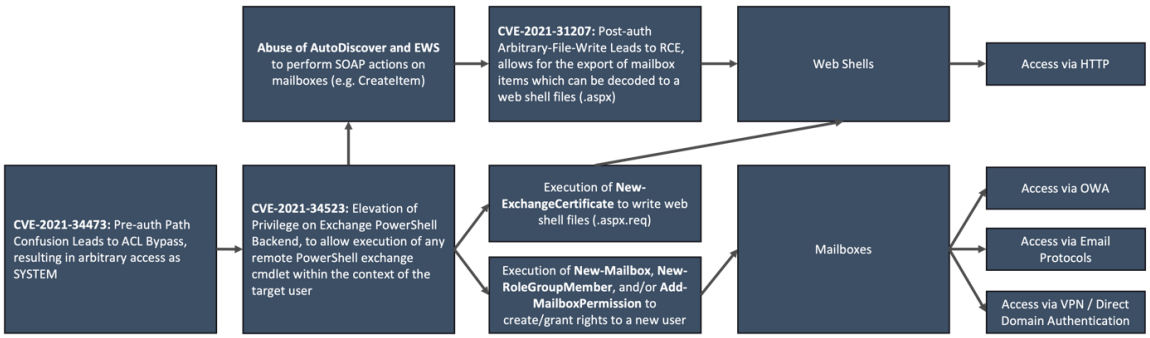

Figure 1: Attack paths

Mandiant has observed multiple actions on objectives originating from these attack paths, including the browsing of email items and deployment of post-exploitation tooling and ransomware.

New-MailboxExportRequest to Write a Web Shell

The widely reported attack path to achieve a web shell is the creation of an item in a target mailbox via Exchange Web Servers (EWS), which Mandiant has observed being a draft email item with an encoded attachment, and subsequent exporting of that item via the New-MailboxExportRequest

cmdlet (after assigning mailbox import/export permissions). The writing of the mailbox item with the specially crafted attachment results in a functional web shell due to the attachment being decoded upon export to the PST file format. This path was demonstrated in the presentation and article by Orange Tsai (@orange_8361) from the DEVCORE Research Team, who discovered and disclosed the exploit chain publicly. Mandiant has observed this path being exploited since August 2021. Refer to Mandiant's previous blog post for further details on this path.

New-ExchangeCertificate to Write a Web Shell

Since September 2021, Mandiant has observed threat actors using the New-ExchangeCertificate cmdlet to save web shell code within a certificate request via the system certificate store. The web shell code is provided to the 'SubjectName' parameter and is saved to disk at a path specified by the 'RequestFile' parameter. Web shells written by this means have been observed on disk with a certificate request extension (.aspx.req). Figure 2 provides an example of the cmdlet executed to achieve this.

```
New-ExchangeCertificate -GenerateRequest "True" -RequestFile "\\ExchangeServer\C$\Program
Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\webshell.aspx" -
SubjectName "<Web Shell Code>" -BinaryEncoded "True" -DomainName ("domain.com")
```

Figure 2: New-ExchangeCertificate cmdlet to write a web shell

Mandiant has identified previous evidence of compromise by searching for web shell code within the system certificate store in the Windows registry (Figure 3), which had persisted after PowerShell logs had rolled over.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\REQUEST\Certificates\<Certificate
Thumbprint/ID>\Blob
```

Figure 3: Registry key for certificate requests in the certificate store

Creation of New Mailboxes and Assigning of Permissions to Access Other Mailboxes

Since August 2021, Mandiant has observed threat actors creating new mailboxes via the New-Mailbox cmdlet then assigning privileged roles via the Add-RoleGroupMember cmdlet, or explicitly assigning full access permissions to other mailboxes with the Add-MailboxPermission cmdlet. In some cases, Mandiant has also observed threat actors hiding these newly created mailboxes from Exchange address lists via execution of the Set-Mailbox cmdlet, with the parameter 'HiddenFromAddressListsEnabled' set to True.

Mandiant has observed actor-controlled mailboxes being used to access other mailboxes via Outlook Web Access (OWA). With the mailbox credentials to new mailboxes being set by the actor, they can also access via other means configured within the environment too, such as through an email client, however Mandiant has not directly observed access by this means.

In configurations where Exchange split permissions (Active Directory split permissions model) are not configured, Mandiant has observed the New-Mailbox cmdlet creating user objects within Active Directory. Where this occurs, threat actors may be able to authenticate with the wider domain or services which use domain authentication, for example corporate VPN's, file sharing platforms, software development platforms, or knowledge management applications. Mandiant has not directly observed access by this means.

Monitoring and Investigating

Mandiant recommends monitoring or investigating for compromise on presently or previously vulnerable Exchange servers.

The monitoring and investigation points in Mandiant's previous blog post still apply, including investigating remote creation of items in mailboxes for exploit by New-MailboxExportRequest, and remote unauthenticated PowerShell for all other attack paths.

Updates to monitoring and investigation based on the observations in this post are as follows:

- New-ExchangeCertificate to write a web shell
  - Execution of the New-ExchangeCertificate PowerShell cmdlet where 'RequestFile' contains a web file extension (.ASPX), or 'SubjectName' contains web shell code, indicating an attempt to drop a web shell via a new certificate request
  - Identification of files with the extension '.ASPX.REQ', indicating a certificate request file saved as an ASPX
  - Identification of web shell code within the decoded system certificate store Blob values on Exchange servers (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\REQUEST\Certificates\<Certificate Thumbprint/ID>\Blob)
- Creation of new mailboxes and assigning of permissions to access other mailboxes
  - Execution of the New-Mailbox PowerShell cmdlet not linked to legitimate administrative activity, or originating from remote unauthenticated PowerShell
  - Identification of unauthorized accounts assigned 'Organization Management' or 'Application Impersonation' roles, or assigned 'Full Access' to other mailboxes
  - Identification of unauthorized accounts hidden from the Exchange address lists
  - Identification of unauthorized access via OWA or other means of email access

Prevention and Remediation

The prevention and remediation guidance from Mandiant's previous blog post still applies, including most crucially applying patches for the vulnerabilities.

Where unauthorized accounts or web shells are identified, Mandiant recommends a full investigation to identify threat actor access in the environment both on the Exchange infrastructure and within the wider domains.

Acknowledgements

Adrian Sanchez Hernandez, Ashely Zaya, Govand Sinjari, Mathew Potaczek, Nick Richard, Yash Gupta