JUMPSEC

Assure | Advise | Respond

UPDATED VULNERABILITY REMEDIATION GUIDANCE FOR MICROSOFT EXCHANGE SERVER

URGENT: Updated Vulnerability Remediation Guidance for Microsoft Exchange Server

Summary: A number of vulnerabilities were recently announced for Microsoft Exchange Server. Threat actors have chained these vulnerabilities together in Exchange to achieve remote code execution in the underlying operating system. Threat actors are actively exploiting this in the wild. Patches have been released which we advise are deployed immediately.

Affecting: Exchange Server 2010, 2013, 2016, and 2019 are affected. Exchange 2010 is affected by CVE-2021-26857 only. Other versions are fully affected by all four vulnerabilities. Exchange Online systems are not affected.

CVEs: 2021-26855, 2021-26857, 2021-26858, 2021-27065

JUMPSEC's Updated Observations and Recommendations:

While patches have been released there have been a number of challenges that JUMPSEC has identified when supporting clients with investigations to locate areas of vulnerability, identify potential exploitation, and deploy remediations, including:

- On March 2nd, communications by Microsoft first claimed that Exchange Server 2010 was unaffected. JUMPSEC's original guidance issued March 2nd advised that organisations also investigate Exchange 2010 due to architectural similarities. On March 3rd this guidance was updated to confirm that Exchange 2010 is vulnerable to CVE-2021-26857 and a patch was released. This miscommunication may have impaired the response efforts of affected organisations.
- When installing the patch for all versions of Exchange Server, some files are not correctly updated when not running as administrator. When this issue occurs, no error message or any indication that the security update was not correctly installed will appear. Further, JUMPSEC notes that not all administrator accounts will possess the correct level of permissions, requiring specific Exchange administrator rights.
- Organisations running third party tooling and scripts should be aware of scenarios where false negatives have been reported due to insufficient read permissions.

For this reason, **JUMPSEC recommends that organisations:**

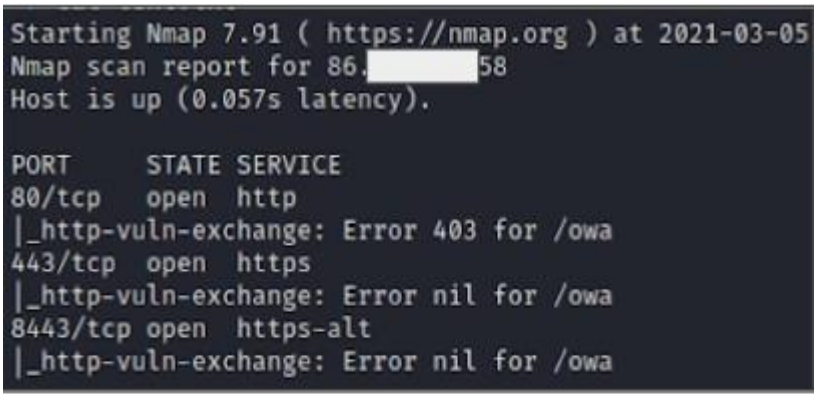
- Check that patches have been installed correctly, and where appropriate implement the steps above.
- Run the latest versions of tooling and scripts where appropriate as many have been subsequently updated and may have provided false assurance that no instances of the vulnerability or IoCs exist when first run.

Given the evolving nature of the situation, JUMPSEC recommends that organisations continue to monitor public feeds (examples provided below) for new intelligence and tooling updates where issues are discovered, and new IoCs emerge. **JUMPSEC consultants are available should you need any advice or support at this time.**

Vulnerability and IoC Identification Guidance:

We have noticed there have been errors in how **nmap** has been used to test a server's vulnerability to Proxylogon.

- These errors have resulted in false negatives.
- When running these scripts, they will clearly say "vulnerable" or "not vulnerable". Therefore please do not interpret "error" to mean "not vulnerable". (we have included a screenshot below of this false negative)
- We have included below a short brief on how to best run nmap to achieve accurate results.



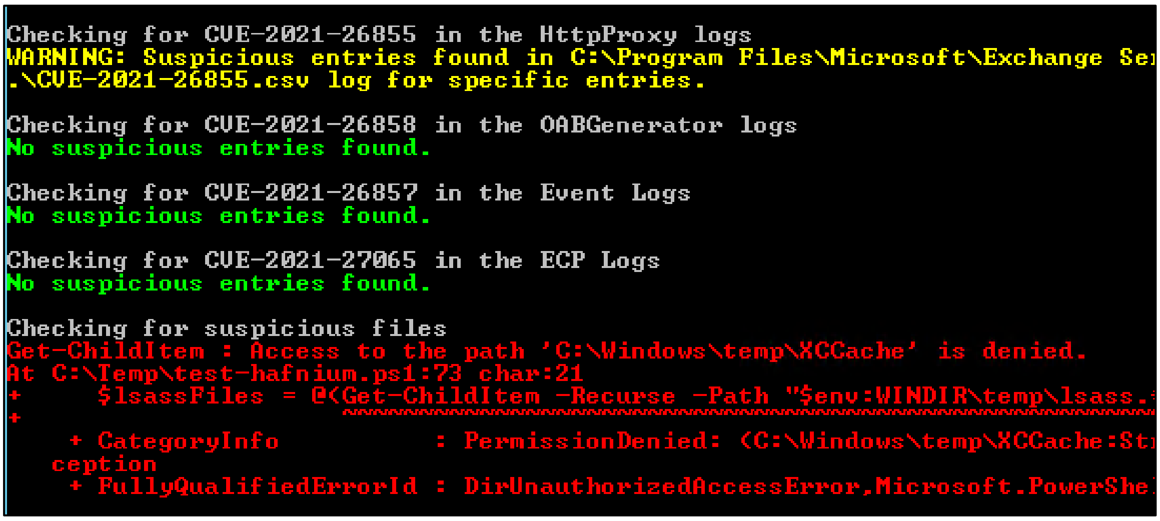
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-05
Nmap scan report for 86.[redacted]58
Host is up (0.057s latency).

PORT     STATE SERVICE
80/tcp   open  http
|_http-vuln-exchange: Error 403 for /owa
443/tcp  open  https
|_http-vuln-exchange: Error nil for /owa
8443/tcp open  https-alt
|_http-vuln-exchange: Error nil for /owa
```

Using **nmap** to determine your vulnerability:

- Download the nmap scripts for ProxyLogon. Currently two are recommended can be run one after another, for confirmation:
  - scanning/http-vuln-exchange.nse at main · GossiTheDog/scanning
  - CSS-Exchange/http-vuln-cve2021-26855.nse at main · microsoft/CSS-Exchange
- Put both of these nmap scripts into the directory: /usr/share/nmap/scripts/
- To run the nmap scripts, these are the basic syntaxes. Add to your nmap script how you see fit, with the specific ports your Exchange runs on:
  - nmap [target] --script http-vuln-exchange.nse --min-rtt-timeout 3
  - nmap [target] --script http-vuln-cve2021-26855.nse

Identifying errors in **IoC powershell scripts**:

- The below screenshot demonstrates that the user who ran the script did not have the necessary permissions to enter directories or read files. This means that the IoC script did not search everywhere for malicious artefacts, and therefore the server could in fact be compromised.



```
Checking for CVE-2021-26855 in the HttpProxy logs
WARNING: Suspicious entries found in C:\Program Files\Microsoft\Exchange Se
.\CVE-2021-26855.csv log for specific entries.

Checking for CVE-2021-26858 in the OABGenerator logs
No suspicious entries found.

Checking for CVE-2021-26857 in the Event Logs
No suspicious entries found.

Checking for CVE-2021-27065 in the ECP Logs
No suspicious entries found.

Checking for suspicious files
Get-ChildItem : Access to the path 'C:\Windows\temp\XCCache' is denied.
At C:\Temp\test-hafnium.ps1:73 char:21
+     $lsassFiles = @(Get-ChildItem -Recurse -Path "$env:WINDIR\temp\lsass.
+                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\temp\XCCache:St
   ception
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShe
```

- We suggest that you run this script as a user with necessary permissions. This may be administrator. However, confusingly, not every administrator is an Exchange administrator. An advisable solution is to create a temporary admin who has recursive read permissions from C:\ onwards. This temporary admin **must** be decommissioned once the script has been run, otherwise this presents a security risk.

Useful Resources:

- Collection of useful resources simplified and collated in one place: Microsoft Exchange Zero Day's - Mitigations and Detections.
- Useful vulnerability identification script: https://github.com/microsoft/CSS-Exchange/blob/main/Security/Test-ProxyLogon.ps1
- Nmap scripts:
- scanning/http-vuln-exchange.nse at main · GossiTheDog/scanning
- CSS-Exchange/http-vuln-cve2021-26855.nse at main · microsoft/CSS-Exchange
- Bash & Powershell regex greps to find IoCs: https://gist.github.com/ecapuano/13386852fb80beac4561f2bed569095e#file-gistfile1-txt
- Scan for HAFNIUM Exploitation Evidence with THOR Lite: Scan for HAFNIUM Exploitation Evidence with THOR Lite
- Reddit feed featuring regular updates (we have found this to be a good source of intelligence): https://www.reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers/

Give us a call
call. 0333 939 8080

Send us a message
email. hello@jumpsec.com

Our address
Unit 3E - 3F, 33 - 34 Westpoint,
Warple Way, Acton, W3 0RG

JUMPSEC

Assure | Advise | Respond

www.jumpsec.com