Microsoft Exchange Breach in Jan. 2021

By By: Nitesh Surana Apr 14, 2021 Read time: 5 min (1258 words)

Published: 2021-04-14 · Archived: 2026-04-05 14:23:33 UTC

Could the Microsoft Exchange breach be stopped?

A look at the latest Microsoft zero-day exploits and how Trend Micro could help protect you.

Last March it seemed the world came to a stand-still as the COVID-19 pandemic begin to rapidly spread. While businesses, sporting events, and schools started shutting down, cybercriminals remained active as ever. In 2020, the Trend Micro Zero Day Initiative™ (ZDI) published 1,453 advisoriesopen on a new tab, the most ever in the history of the program. More startling is the fact that 18.6% of all disclosures were published without a fix from the vendor—another record-breaking stat.

As ZDI predicted, 2021 continued to be a busy year. In March 2021, Microsoft kicked off the patch cycle early after releasing an advisoryopen on a new tab regarding the mass exploitation of four zero-days vulnerabilities by a Chinese Hacking group, HAFNIUM, on the on-premises versions of the Microsoft Exchange Server. In the following days of the attack, Trend Micro reported that at least 30,000 organizations were thought to have been attacked in the US, and 63,000 servers remained exposed to these exploits.

The vulnerability has been dubbed as ProxyLogonopen on a new tab by the researchers at DEVCORE, who are credited with finding the bugs in the proxy architecture and the logon mechanism of Exchange. DEVCORE reported two of the four zero-days (CVE-2021-26855open on a new tab and CVE-2021-27065open on a new tab) to Microsoft Security Response Center (MSRC). On March 2, Volexityopen on a new tab reported in-the-wild exploitation of the vulnerabilities, to which DEVCORE confirmedopen on a new tab that the exploit observed by Volexity was the one submitted to MSRC.

Since then, there has been opportunistic exploitation by various threat actors and ransomware groups (Dearcry, BlackKingdom) since majority of Outlook Web App portals are public and indexed by search engines like Google Search, Shodan, Binaryedge, Censys, Zoomeye etc. According to Shodanopen on a new tab, on March 4, there were more than 266,000 Exchange Servers vulnerable to the ProxyLogon vulnerability, a day after the patch was released.


Shodan Results

Fig - Shodan Results

In lieu of these exploits, let’s take a look at how Trend Micro Vision One™ and Trend Micro Cloud One™ can provide protection against two of the four zero-days, CVE-2021-26855 and CVE-2021-27065.

Overview:
Two bugs are chained to achieve the remote code execution and for the attack to be successful, an attacker

requires access to the Outlook Web App portal of the vulnerable Exchange Server, and a valid email address.

1. CVE-2021-26855: Microsoft Exchange Server Remote Code Execution Vulnerability (pre-authenticated Server-Side Request Forgery [SSRF])
2. CVE-2021-27065: Microsoft Exchange Server Remote Code Execution Vulnerability (post-authenticated Arbitrary File Write)

Fig - MS Exchange Client Access Protocol Architecture

The Client Access services (Outlook Web App portal) proxies the incoming connections to the Backend services. As per the Exchange documentationopen on a new tab, clients don't directly connect to the backend services. But because of the SSRF vulnerability, attackers can query the internal backend services and APIs on the Exchange Server, bypassing the frontend proxy.

By abusing the SSRF, attackers can create session IDs and access tokens for privileged accounts with the context of the Exchange Control Panel, which can be used to write files with attacker-controlled content at a location on the target server, chosen by the attacker. Since Exchange depends on Internet Information Services (IIS) webserver, an attacker can write ASPX webshells and run arbitrary commands as SYSTEM on the Exchange Server.

In January 2021, we came across extensive use of Chopper ASPX webshells in targeted attacks by malicious actors to establish persistence and a foothold on the public-facing Outlook Web App servers.

Trend Micro Cloud One™ – Workload Security Correlation:
Trend Micro Cloud One™ – Workload Security is a cloud-native solution that provides automated security via powerful APIs. Security as code allows DevOps teams to bake security into their build pipeline to release continuously and frequently, so developers like yourself, can keep working without disruption from security. Workload Security uses advanced security controls such as intrusion prevention system (IPS), deep packet inspection (DPI), and integrity monitoring to protect Exchange Servers from attackers that could exploit ProxyLogon. The following detection rules safeguard a vulnerable Exchange Server from the CVEs reported:

Intrusion Prevention System detections:

1. 1010854 - Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-26855)
2. 1010868 - Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-27065)
3. 1010870 - Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-27065) – 1
4. 1007170 - Identified Suspicious China Chopper Webshell Communication (ATT&CK T1100)
5. 1005934 - Identified Suspicious Command Injection Attack

Integrity Monitoring detections:

1. 1010855 - Microsoft Exchange - HAFNIUM Targeted Vulnerabilities

1010854 - Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-26855)

1007170 - Identified Suspicious China Chopper Webshell Communication (ATT&CK T1100)

1007170 - Identified Suspicious China Chopper Webshell Communication (ATT&CK T1100)

1010870 - Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-27065) - 1

1010870 - Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-27065) - 1

1005934 - Identified Suspicious Command Injection Attack

1005934 - Identified Suspicious Command Injection Attack

1010855 - Microsoft Exchange - HAFNIUM Targeted Vulnerabilities

1010855 - Microsoft Exchange - HAFNIUM Targeted Vulnerabilities

Trend Micro Vision One™ Correlation:

Microsoft Exchange Server RCE Vulnerability (CVE-2021-26855 + CVE-2021-27065)

Fig - Microsoft Exchange Server RCE Vulnerability (CVE-2021-26855 + CVE-2021-27065)

Trend Micro Vision One™ is a purpose-built, threat defense platform with extended detection and response (XDR) capabilities that work to prevent majority of attacks with automated protection. The solution allows you to see more and respond faster by collecting and correlating data across email, endpoints, servers, cloud workloads, and networks.

Using the Trend Micro Vision One Workbenchopen on a new tab, you can easily see what threats were detected, attack techniques, and a prioritized list of risky devices and users. With Trend Micro Vision One, we ran a public proof of concept (PoC) availableopen on a new tab online exploiting the ProxyLogon vulnerability. The above image shows the vulnerability detected and all the assets related to the alert for further investigation. Let’s take a deeper look:

Potential Chopper Webshell Detection

Fig - Potential Chopper Webshell Detection

The Potential Chopper Webshell Execution model triggers when the web shell is already present on the machine and is being used as a backdoor to run commands as SYSTEM on the Exchange Server using China Chopper.

The metrics provided by this model should be investigated carefully, since the ProxyLogon zero-day vulnerability was exploited in-the-wild, before Microsoft addressed the issue publicly. Microsoft has since taken things a step further by creating patchesopen on a new tab for out-of-support versions of Exchange. Overall, Microsoft released patches for 89 unique CVEs in March—14 of which were listed as Critical and 75 listed as Important in severity.

Fig - Microsoft Exchange Server Possible ASPX Web Shell

The above model triggers when a new web shell is created. You can see the path and name of the web shell.

Fig - Potential Chopper Webshell Execution

Fig - Identified Suspicious China Chopper Webshell Communication

Fig - Possible Credential Dumping via Command Line

This model is triggered when an attacker fetches the credentials using a command-line from within the memory using Mimikatz. Since the web shell runs as the SYSTEM user, an attacker can fetch the NT LAN Manager (NTLM) hashes of the logged-in users, create or delete accounts, and perform extensive post-exploitation activities on the Exchange Server.

Figure - Executing Mimikatz as SYSTEM using CC

Fig - System Owner User Discovery

The above event was triggered when we ran whoami from within the Chopper web shell. Since requests to the ASPX web shell are handled by the privileged w3wp.exe, an IIS Worker Process in the configured IIS application pool (Microsoft Exchange App pool) runs the commands in the context of NT Authority\SYSTEM user.

RCA Diagrams:

Fig. Executing commands using Chopper CnC

Conclusion

There is no silver bullet when it comes to cybersecurity but using solutions that bake into your development pipeline to provide security as early as possible is better than scrambling for patches after deployment. Quick and easy to deploy solutions like Trend Micro Cloud One and Trend Micro Vision One can provide you with SecOps-approved security from build-time to runtime without slowing you down. Imagine that!

Tags
