THREAT BULLETINS

Weaponized ProxyShell Vulnerability Targeting Microsoft Exchange Servers

TLP:WHITE

Aug 26, 2021

Microsoft and the US Cybersecurity and Infrastructure Security Agency (CISA) have issued two separate alerts regarding the weaponization and the successful exploitation of three security flaws in Microsoft Exchange designated ProxyShell. Several security firms have observed several attacks targeting vulnerable instances of Micrsoft Exchange that have not applied Microsoft patches KB5001779 and KB5003435.

The Health-ISAC Theat Operations Center has linked both the CISA and Microsoft advisory for your heightened security awareness and endorses the subsequent mitigation strategies recommended by Microsoft and CISA.

ProxyShell is a collection of three security flaws discovered by a Devcore security researcher, who exploited them to compromise a Microsoft Exchange server during the Pwn2Own 2021 hacking contest.

The three vulnerabilities are listed below:

- CVE-2021-34473 - Pre-auth path confusion leads to ACL Bypass (Patched in April by Microsoft KB5001779)
- CVE-2021-34523 - Elevation of privilege on Exchange PowerShell backend (Patched in April by Microsoft KB5001779)
- CVE-2021-31207 - Post-auth Arbitrary-File-Write leads to RCE (Patched in May by Microsoft KB5003435)

After additional technical details were disclosed by the researcher, other security researchers and threat actors eventually reproduced a working ProxyShell exploit. Less than two months later, attackers began scanning for and hacking Microsoft Exchange servers using their newly crafted ProxyShell exploit. After breaching unpatched Exchange servers, threat actors have the ability to drop web shells that allow them to further upload and execute malicious tools.

Even though Microsoft fully patched the ProxyShell vulnerabilities in KB5001779 and KB5003435, they didn't assign CVE IDs for the three security vulnerabilities until late July, preventing some organizations who had unpatched servers from discovering that they had vulnerable systems on their networks. Huntress Labs has stated that it has now seen over 140 malicious web shells installed across over 1900 unpatched servers via ProxyShell over the last week.

According to the CISA report, malicious cyber actors are actively exploiting ProxyShell vulnerabilities. Microsoft has also released a separate report stating that customers must install at least one of the supported latest cumulative updates and all applicable security updates to block ProxyShell attacks.

Reference(s)	Microsoft, Microsoft, Bleeping Computer, Microsoft, Microsoft, Microsoft, Microsoft, Twitter, Twitter

Recommendations
CISA and Microsoft have both strongly urged organizations to identify vulnerable systems on their networks and immediately apply Microsoft's Security Update KB5001779 and KB5003435.

The US National Security Agency (NSA) has also reminded defenders that previous guidance published in March on hunting for web shells is still applicable to these ongoing attacks, which can be accessed here.

Sources
CISA: Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities

Microsoft: ProxyShell Vulnerabilities and Your Exchange Server

NSA: Detect and Prevent Web Shell Malware

BleepingComputer: CISA Warns Admins to Urgently Patch Exchange ProxyShell Bugs

BleepingComputer: Microsoft: ProxyShell Bugs Might Be Exploited Patch Servers Now!

Alert ID 412c2e51

View Alert

Tags KB5003435, KB5001779, ProxyShell vulnerability, ProxyShell, ProxyShell remote code execution flaws, ProxyShell Vulnerabilities, Microsoft Exchange Bugs, Microsoft Exchange Server, Microsoft Exchange

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.


If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.