Radware Cybersecurity Advisory

ProxyLogon: Zero-Day Exploits In Microsoft Exchange Server

March 16, 2021

A series of new zero-day exploits in Microsoft Exchange Servers discovered late last year has evolved into a global hacking spree now impacting hundreds of thousands of organizations worldwide.

On March 2, Microsoft released critical security updates for four crucial zero-day vulnerabilities discovered in Exchange Servers and reported that the exploits are being actively exploited by an actor called HAFNIUM, a state-sponsored group operating out of China.

Within one week, at least 30,000 U.S. organizations and hundreds of thousands of organizations worldwide have fallen victim to an automated campaign run by HAFNIUM that provides the attackers with remote control over the affected systems.

In the past week, the patched vulnerabilities have been weaponized by over 10 different APT groups and are being leveraged in ransomware and cryptomining campaigns.

Threat Assessment

Radware assesses the threat as critical for all industries across the globe, from small to large corporations. Initial reports indicated the involvement of advanced Chinese actors. Chinese APT groups are known for espionage and targeting governments, pharmaceutical/research institutions, research in general and corporate research assets.

Last week, exploits started to circulate and ransomware and cryptocurrency campaigns started exploiting the vulnerabilities. Consequently, the threat is now generic and global, putting any organization, independent of industry or location, at risk of falling victim to ransomware and cryptomining abuse.

ProxyLogon

On December 10, 2020, Orange Tsai, a researcher working for the Taiwanese security consulting organization **DEVCORE**, discovered a pre-authentication proxy vulnerability (CVE-2021-26855) in Exchange Servers that allows a remote actor to bypass authentication and receive admin server privileges. Combined with a post-authentication vulnerability (CVE-2021-27065) that allows arbitrary file writes to the system (discovered by Tsai three weeks later), an actor can achieve remote command execution of arbitrary commands through internet-exposed Exchange Servers. Initial access is achieved through uploading a web shell, commonly referred to as a "**China chopper**."

CVE-2021-26855: SERVER SIDE REQUEST FORGERY

The Server-Side Request Forgery (SSRF) vulnerability provides a remote actor with admin access by sending a specially crafted web request to a vulnerable Exchange Server. The web request contains an XML SOAP payload directed at the Exchange Web Services (EWS) API endpoint. The SOAP request bypasses authentication using specially crafted cookies and allows an unauthenticated, remote actor to execute EWS requests encoded in the XML payload and ultimately perform operations on users' mailboxes. This vulnerability, combined with the knowledge of a victim's email address, means the remote actor can exfiltrate all emails from the victim's Exchange mailbox.

CVE-2021-26857: REMOTE CODE EXECUTION VULNERABILITY

A post-authentication insecure deserialization vulnerability in the Unified Messaging service of a vulnerable Exchange Server allows commands to be run with SYSTEM account privileges. The SYSTEM account is used by the operating system and services that run under Windows. By default, the SYSTEM account is granted full control permissions to all files. A malicious actor can combine this vulnerability with stolen credentials or with the previously mentioned SSRF vulnerability to execute arbitrary commands on a vulnerable Exchange Server in the security context of SYSTEM.

CVE-2021-26858 AND CVE-2021-27065

Both of these post-authentication arbitrary file write vulnerabilities allow an authenticated user to write files to any path on a vulnerable Exchange Server. A malicious actor could leverage the previously mentioned SSRF vulnerability to achieve admin access and exploit this vulnerability to write web shells to virtual directories (VDirs) published to the internet by the server's Internet Information Server (IIS). IIS is Microsoft's web server, a dependency that is installed with Exchange Server and **provides** services for Outlook on the web, previously known as Outlook Web Access (OWA), Outlook Anywhere, ActiveSync, Exchange Web Services, Exchange Control Panel (ECP), the Offline Address Book (OAB) and Autodiscover.

Active Exploitation

On March 2, Volexity **reported** seeing active exploitation of multiple Microsoft Exchange vulnerabilities. Several vulnerabilities were chained together and used to steal email and compromise networks as early as January 6. Volexity later confirmed the vulnerabilities to be the SSRF (CVE-2021-26855) chained with the arbitrary file writing (CVE-2021-27065), also known as ProxyLogon.

That same day, Microsoft **reported** it had detected multiple zero-day exploits in Exchange Servers in limited and targeted attacks. In the observed attacks, an advanced actor leveraged the vulnerabilities to access email accounts and install additional malware to facilitate long-term access to their victims. Microsoft Threat Intelligence Center (MSTIC) attributed this campaign based on observed victimology, tactics and procedures, with high confidence to **HAFNIUM**, a group assessed to be state-sponsored and operating out of China.

On March 5, KrebsonSecurity **reported** on the unusually aggressive Chinese cyber-espionage unit that was exploiting the vulnerabilities and had seeded hundreds of thousands of victim organizations worldwide and at least 30,000 organizations across the U.S. with tools that give the attackers total and remote control over the affected systems.

The European Banking Authority (EBA) **disclosed** a cyberattack targeting its Microsoft Exchange Servers on March 7.

Lawrence Abrams from BleepingComputer **reported** on a new ransomware dubbed DearCry that victims started reporting as early as March 9. Microsoft later confirmed that the DearCry ransomware is installed through human-operated attacks on Microsoft Exchange Servers using the ProxyLogon vulnerabilities.

Palo Alto Networks' Unit42 **estimated** that 125,000 unpatched Exchange Servers remain exposed on the internet by March 9.

On March 10, ESET Research **uncovered** at least 10 APT groups exploiting ProxyLogon and planted web shells on more than 5,000 Exchange Servers.

By March 12, BleepingComputer **reported** that the operators of Lemon_Duck, a cryptomining botnet that targets enterprise networks, started using the ProxyLogon exploits in an attempt to install their XMRig Monero (MXR) coinminer in vulnerable servers.

In the past week, proof of concepts for the SSRF exploit started to appear. Microsoft **removed** the first publication of a purposely broken example on Github. However, as more people began to share and republish, ultimately, fully functioning examples made their way to the most popular code-sharing repositories. The exploit is now within reach of everyone that wants to abuse it.

Until March 15, the Radware Global Deception Network recorded only two isolated global random scans for exposed Exchange Servers (see Figure 1 below). There is reason to believe the random scanning will increase in the coming days as more malicious actors integrate the working proof of concepts in their existing campaigns and botnets.

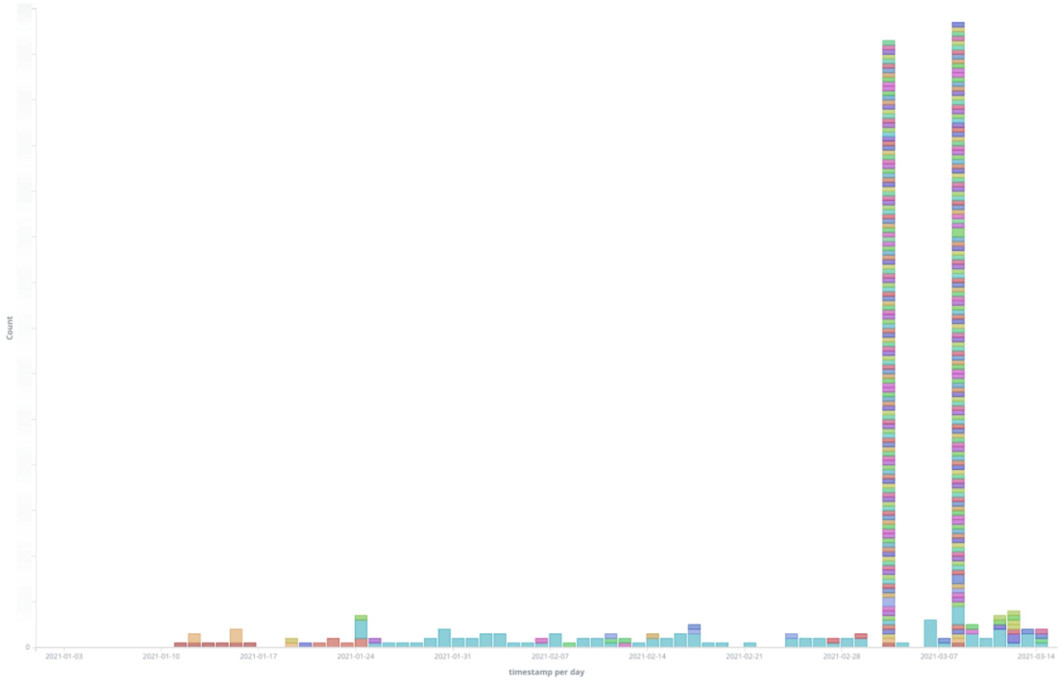

Figure 1: Exchange Server Scanning attempts; source: Radware Global Deception Network

Mitigation

Any Microsoft Exchange Server 2013, 2016, or 2019 that is or was exposed to the internet after January 1, 2021 and able to receive untrusted connections, is potentially compromised. Exchange Online is not affected by the vulnerabilities.

Exchange Server 2010 is only affected by CVE-2021-26857 and as such not impacted by the initial access SSRF vulnerability. However, it is strongly recommended to install the latest security updates.

Exchange Server 2003 and 2007 are not supported anymore and should be upgraded to a newer, supported version of Exchange as soon as possible.

Microsoft has provided **interim mitigations** for organizations that are unable to upgrade immediately or need more time to pass quality assurance testing. The mitigations are based on the implementation of IIS re-write rules and disabling Unified Messaging, the Exchange Control Panel VDir and the Offline Address Book VDir.

Radware provides interim protection for the pre-authentication vulnerabilities CVE-2021-26855 and CVE-2021-26857 through threat signatures RWID 19888 through 19894. The signatures are published and automatically activated through our ERT Security Update Subscription (SUS).

After updating or protecting the Exchange Server, it is still strongly advised to check for traces of potential earlier exploits that could have happened during the timeframe between the first attacks and the updates. Microsoft released a PowerShell **script** that can detect the presence of web shells.

Even if no web shells were detected, a broader forensic audit is still recommended. Start by sifting through Exchange web server logs for traces of command executions which can be accomplished leveraging the PowerShell scripts that have been made public by the security community.

Finally, it is important to ensure no data was exfiltrated or accounts compromised or added by malicious actors. Even when no traces of compromise were detected on the server, malicious actors could have wiped their trail while still maintaining a foothold.

Resources and References

1. Microsoft Advisory: **https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/**
2. Microsoft Security Blog - Hafnium targeting Exchange Servers: **https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/**
3. Volexity Blog: **https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/**
4. Microsoft blog on Exchange Server Vulnerabilities Mitigations: **https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/**

5. ProxyLogon: https://proxylogon.com/
6. Ransomware now attacks Microsoft Exchange servers with ProxyLogon exploits: https://www.bleepingcomputer.com/news/security/ransomware-now-attacks-microsoft-exchange-servers-with-proxylogon-exploits/
7. Breaking Down the China Chopper Web Shell - Part I | FireEye Inc: https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
8. At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's E-mail Software — Krebs on Security: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/
9. Cyber-attack on the European Banking Authority | European Banking Authority: https://www.eba.europa.eu/cyber-attack-european-banking-authority
10. Exchange servers under siege from at least 10 APT groups | WeLiveSecurity: https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
11. Remediation Steps for the Microsoft Exchange Server Vulnerabilities: https://unit42.paloaltonetworks.com/remediation-steps-for-the-microsoft-exchange-server-vulnerabilities/

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** using negative and positive security models for maximum accuracy
- **Auto-policy generation** capabilities for the widest coverage with the lowest operational effort

- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit Radware's Security Center. It is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.