NORTH CAROLINA'S
INFORMATION SHARING AND ANALYSIS CENTER
ISAAC

SITUATIONAL AWARENESS BULLETIN

UNCLASSIFIED//TLP:WHITE

March 12, 2021

(UNCLASSIFIED // TLP:WHITE)

Microsoft Exchange Server Vulnerability Guidance

This information has been compiled by the
the North Carolina Joint Cybersecurity Task Force

Situation

Beginning in January 2021, Mandiant Managed Defense observed multiple instances of abuse of Microsoft Exchange Server within at least one client environment. The observed activity included creation of web shells for persistent access, remote code execution, and reconnaissance for endpoint security solutions. On March 2, 2021, Microsoft released a blog post that detailed multiple zero-day vulnerabilities used to attack on-premise versions of Microsoft Exchange Server. Microsoft also issued emergency Exchange Server updates for the following vulnerabilities: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065

Microsoft attributed the original compromise to a Chinese state-sponsored threat actor HAFNIUM. However, since the exploits became publicly available in early March, there have been at least 10 threat groups exploiting the vulnerabilities according to the cybersecurity company ESET. Based on ESET's telemetry, web shells have already been deployed on over 5,000 unique Exchange Servers from over 115 countries. FireEye currently tracks this activity in three clusters, UNC2639, UNC2640, and UNC2643. They anticipate additional clusters as they respond to intrusions. It is recommended to follow Microsoft's guidance and patch Exchange Servers immediately to mitigate this activity.

The main vulnerabilities known to be exploited are as follows:

CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange which allowed the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.

CVE-2021-26857 is an insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialized by a program. Exploiting this vulnerability gave the threat actor the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit.

CVE-2021-26858 is a post-authentication arbitrary file write vulnerability in Exchange. If the threat actor could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

CVE-2021-27065 is a post-authentication arbitrary file write vulnerability in Exchange. If the threat actor could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

Definitions

Patched	Exchange Server has been Patched
Exposed	Exchange server has not been patched and is vulnerable but, no IOCs have been identified on the network
Compromised	IOCs associated with the vulnerability have been observed in the network
Threat Hunting	Threat hunting is the act of searching a network to determine if a compromise has occurred
Remediated	Exchange Server has been patched, and threat hunting has been completed. If compromise was identified the system has been cleared

Industry Best Practices

The exploitation of Microsoft Exchange on-premise products poses an extremely high risk to Federal Civilian Executive Branch agencies, SLTT government entities and private sector organizations and requires emergency action. This determination is based on the current exploitation of these vulnerabilities in the wild, the likelihood of the vulnerabilities being exploited, the prevalence of the affected software in the federal enterprise, the high potential for a compromise of information systems, and the potential impact of a successful compromise.

1. After identifying all instances of on-premise Microsoft Exchange Servers in the environment, organizations that have the expertise should forensically triage artifacts using collection tools (see CISA's Activity Alert and the Resources section of this document for examples) to collect system memory, system web logs, windows event logs, and all registry hives. Organizations should then examine the artifacts for indications of compromise or anomalous behavior, such as credential dumping and other activities as described in the Activity Alert. Organization should simultaneously apply patches to the server. If there is anomalous behavior or an indication of compromise detected, proceed to Action 2.
If no indications of compromise have been found, organizations should immediately apply Microsoft patches for Microsoft Exchange servers. If an organization does not have the expertise to forensically triage its systems, it should proceed to Action 3.

2. Organizations that have the expertise to take the following steps immediately should do so before proceeding to Action 3. Organizations should examine artifacts collected in this step for indications of compromise or anomalous behavior, such as credential dumping, lateral movement, persistence mechanisms and other follow on exploitation activity. Organizations without this expertise shall proceed to Action 3.

    a. Forensically image system memory or, for virtual hosts, make a copy of the Virtual Memory (VMEM) to external storage for analysis.

b. If a live forensic disk image can be acquired, follow procedures to acquire the live system disk image.
c. If a live forensic disk image cannot be acquired, pause all instances of systems (virtual machines) running Outlook on the Web a.k.a. Outlook Web Access/App (collectively OWA) or Exchange Control Panel (ECP).
d. Conduct forensic analysis of the system memory and disk image to look for IOCs provided in CISA Activity Alert
e. Analyze stored network traffic and metadata for indications of compromise provided in the CISA Activity Alert, or suspicious connections.
f. Hunt the network and systems for additional indications of compromise, which are provided in CISA Activity Alert and in the Reference section of this document.

3. Organizations that have identified indications of compromise in Action 1, or did not have the expertise to conduct Action 1 or 2, should follow these steps and proceed to Action 4:
   a. Immediately disconnect Microsoft Exchange on-premises servers.
   b. Until Microsoft Exchange Server operating systems are rebuilt and the software package is reinstalled, organizations should refrain from (re)joining the Microsoft Exchange Server to the enterprise domain.
   c. Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.
4. Immediately report as an incident to CISA or to the North Carolina Emergency Management the existence of any of the following:
   a. Identification of indicators of compromise as outlined in CISA Activity Alert.
   b. Presence of web shell code on a compromised Microsoft Exchange on-premises server.
   c. Unauthorized access to or use of accounts.
   d. Evidence of lateral movement by malicious actors with access to compromised systems.
   e. Other indicators of unauthorized access or compromise.
   f. Other indicators related to this issue to be shared by CISA in the Activity Alert.

Reporting

If your organization is exposed and/or compromised and needs further assistance with any of the above recommended industry best practices please contact the Joint Cybersecurity Task Force (JCTF) at the reportspam@ncem.org email.

The JCTF will be following with an organization survey request and any additional information as it becomes available.

Resources

- https://us-cert.cisa.gov/ncas/alerts/aa21-062a
- https://cyber.dhs.gov/ed/21-02/
- https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
- https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- https://cyber.dhs.gov/ed/21-02/
- https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
- https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html

CVEs

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

IOCs

- https://github.com/microsoft/CSS-Exchange/tree/main/Security
- https://us-cert.cisa.gov/sites/default/files/publications/AA21-062A.stix.xml
- https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
- https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/MSTICIoCs-ExchangeServerVulnerabilitiesDisclosedMarch2021.json
- https://github.com/microsoft/CSS-Exchange/tree/main/Security