Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

13 April 2021

PIN Number
AC-20210413-002

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
http://www.fbi.gov/contact-us/field-offices

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This PIN has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

FBI Disrupts Cyber Actors' Exploitation of Microsoft Exchange Server Vulnerabilities

Summary

On 13 April 2021, the Federal Bureau of Investigation (FBI) conducted a court-authorized operation to remove hundreds of malicious web shells from vulnerable servers in the United States in response to the widespread exploitation of critical Microsoft Exchange Server (MES) vulnerabilities by malicious cyber actors. The servers ran on-premises versions of MES, a software used to provide enterprise-level e-mail service. This is unrelated to Microsoft's 13 April announcement of security updates for additional MES vulnerabilities.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Background

As early as January 2021, cyber actors began exploiting zero-day vulnerabilities in MES software to infect the networks with web shells[i] and access email accounts. Compromising a MES could allow threat actors the ability to read sensitive information in the mailboxes of users, steal user credentials, add user accounts, steal copies of network management databases, and move laterally to other systems or environments.

On 2 March 2021, Microsoft announced that multiple zero-day vulnerabilities were used to target computers running MES. Since then, additional cyber actors have attempted to use the same vulnerabilities to place web shells on unpatched computers worldwide. Because each web shell had a unique file path and name, it was more challenging for individual server owners to detect and eliminate them.

Throughout March 2021, Microsoft and other industry partners released detection tools, patches, and other information to assist victim entities in identifying and mitigating this cyber incident. The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) released a Joint Advisory titled "Compromise of Microsoft Exchange Server" on 10 March 2021. Despite these efforts, by the end of March, hundreds of web shells remained on a number of US-based MESs.

The FBI's operation on 13 April 2021 removed certain remaining web shells from as many systems as it was able to in order to prevent adversaries from escalating persistent, unauthorized access to US networks. Additional information on the threat can be found in the "Additional References" section.

What happened?

Following approval by the Department of Justice (DOJ), the FBI conducted a court-authorized operation on 13 April 2021 to search for, copy, and remove malicious web shells that provided backdoor access to vulnerable on-premises[ii] versions of MES in the United States related to CVE-2021-26855,[iii] CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.

---

[i] Web shells are pieces of code or scripts running on a server that enable remote administration.

[ii] The Exchange Server vulnerability zero-days mentioned in the 2 March 2021 Microsoft report only affected on-premises systems and not Exchange Online.

[iii] CVE-2021-26855 is colloquially called ProxyLogon.

However, the operation did not include follow-on mitigating actions, such as patching any MES vulnerabilities or identifying and removing any additional malware or hacking tools the actors may have placed on victim networks through the web shells or that may have already been present on networks.

Technical Details

Although many infected system owners successfully removed the web shells from thousands of computers following the 2 March public notification, others appeared unable to do so, and hundreds of such web shells persisted unmitigated until FBI's operation.

The FBI identified the remaining compromised MESs and conducted a removal by issuing a command through the web shell to the server, deleting the web shell as identified by its unique file path.[iv] By deleting the web shells, the FBI prevented malicious cyber actors from using them to access the servers and install additional malware. The following is an anonymized example of one of the delete commands that was sent through a web shell located at example location, https://webmail.[domain][.]net/aspnet_client/system_web/CEzmlYXD.aspx:

- del /f "C:\inetpub\wwwroot\aspnet_client\system_web\CEzmlYXD.aspx

Recommended Follow-on Actions

The FBI and DOJ strongly encourage network defenders to review Microsoft's remediation guidance and the 10 March 2021 Joint Advisory for further guidance on detection and patching.

If you were a victim and the removal operation was conducted on your system, you will receive additional details from an authorized FBI email account.

If you believe you have a compromised computer running MES, please contact your local FBI field office for assistance. The FBI continues to conduct a thorough and methodical investigation into this cyber incident.

Additional References

The US Government and private cybersecurity industry have published numerous reports concerning the Microsoft Exchange Vulnerabilities and its exploitation by malicious cyber actors.

[iv] While each web shell has a file path ending in a unique string of eight characters, the deleted web shells were identified using the following partial file path: "\inetpub\wwwroot\aspnet_client\system_web."

- CISA Remediating Microsoft Exchange Vulnerabilities web page
- CISA Activity Alert (AA21-062A): Mitigate Microsoft Exchange Server Vulnerabilities
- FBI/CISA Joint Cybersecurity Advisory (AA21-069A): Compromise of Microsoft Exchange Server
- Microsoft Blog: HAFNIUM targeting Exchange Servers with 0-day exploits
- Volexity Blog: Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities
- Splunk Blog: Detecting HAFNIUM Exchange Server Zero-Day Activity in Splunk
- Microsoft Security: Analyzing Attacks Taking Advantage Of The Exchange Server Vulnerabilities

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 CyberWatch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey