Knowledgebase > Server Solutions > Does ESET protect me from the Hafnium zero-day exploit in Microsoft Exchange?

Does ESET protect me from the Hafnium zero-day exploit in Microsoft Exchange?

Steef | ESET Nederland - 2023-01-13 - Comments (0) - Server Solutions

Issue

Your ESET security product detects the following threat:

JS/Exploit.CVE-2021-26855.Webshell.A
JS/Exploit.CVE-2021-26855.Webshell.B
ASP/Webshell
ASP/ReGeorg

This threat affects users of Microsoft Exchange Server versions 2010, 2013, 2016, and 2019

Details

After exploiting vulnerabilities to gain initial access, HAFNIUM operators deployed webshells on the compromised server. Webshells potentially allow attackers to steal data and perform additional malicious actions that lead to further compromise.

For more details see ESET Customer Advisory.

Solution

ESET software can detect and block the webshell used for remote code execution.

The detection for the webshells and backdoors used within this attack chain appears as:

- JS/Exploit.CVE-2021-26855.Webshell.A
- JS/Exploit.CVE-2021-26855.Webshell.B
- ASP/Webshell
- ASP/ReGeorg

The Microsoft Exchange server remote code execution vulnerabilities are:

- CVE-2021-26855 (the most common)
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

Install the Microsoft security patch

ESET strongly advises installing the Microsoft security update immediately.

See Microsoft's article for details on how to install the security update.

See more technical information and attack details on HAFNIUM.

To ensure the highest level of security, we recommend that you are always on the latest version of your ESET product: Check for the latest version of your ESET business products

Keep ESET Live Grid enabled

In some cases, your ESET product with ESET Live Grid enabled may respond faster to new threats than to modules updates.

Click here to learn more about ESET Live Grid and make sure it is enabled in your ESET product.

Minimize the risk of malware attack

What can I do to minimize the risk of a malware attack?

- Back up your important data
- Do not change default settings
- Download security patches

WeLiveSecurity blog post

To learn more about how you can protect your system from this exploit, we recommend that you read the following ESET blog post:

- Microsoft rushes out fixes for four zero-day flaws in Exchange Server
- Exchange servers under siege from at least 10 APT groups

To see a list of all ESET security articles related to zero-day attacks, see zero-day attacks.