Microsoft Patches Exchange Software Flaws Targeted

Microsoft has rolled out a security update to fix four zero-day flaws in Exchange Server that bad actors have been using to infiltrate companies and organizations across industries. A Chinese state-sponsored group called Hafnium has been behind most of the cyberattacks that exploited the vulnerabilities, the tech giant said in a post. Microsoft describes the group as a "highly skilled and sophisticated actor" that primarily targets entities in the United States, including law firms, educational institutions, defense contractors and NGOs.

The group used the vulnerabilities to gain entry into its targets' Exchange Server, the company's mail and calendaring server, account. It then installs a backdoor into their system so it be accessed remotely, and then use that remote access to steal information from its victim. Microsoft says Hafnium conducts its operations primarily from leased virtual private servers in the US despite being based in China.

The tech giant credits researchers at security companies Volexity and Dubex for notifying it about Hafnium's activities and helping it address the issue. In Extreme mining about the vulnerabilities, Volexity said at least one of them does not require authentication of any kind or even any special knowledge or access to a target environment. "The attacker only needs to know the server running Exchange and the account from which they want to extract e-mail," the post reads.

Microsoft has already notified the US government of Hafnium's activities and is encouraging users to install the update. The company clarifies, though, that these particular exploits are in "no way connected to the separate SolarWinds-related attacks."