Microsoft defends against new threat to Exchange

April 14 2021

Credit: Pixabay/CC0 Public Domain

Microsoft on Tuesday moved to defend against a dangerous new threat to Exchange email servers while the fight continued against hackers taking advantage of a flaw patched last month.

The US Cybersecurity and Infrastructure Security Agency, part of the

Department of Homeland Security, called on government departments to immediately install the latest software update released by Microsoft.

"These vulnerabilities pose an unacceptable risk to the Federal enterprise and require an immediate and emergency action," CISA said in a notice.

"This determination is based on the likelihood of the vulnerabilities being weaponized, combined with the widespread use of the affected software across the Executive Branch and high potential for a compromise of integrity and confidentiality of agency information."

Both CISA and Microsoft said it did not appear that hackers had taken advantage of the newly discovered weakness to break into Exchange email systems.

"Although we are not aware of any active exploits in the wild, our recommendation is to install these updates immediately to protect your environment," Microsoft said in a post about the patch.

CISA and Microsoft said that the vulnerabilities were different from those fixed last month, when the US tech company disclosed that a state-sponsored hacking group operating out of China was exploiting security flaws in its Exchange email services to steal data from business users.

The company said the hacking group, which it has named "Hafnium," is a "highly skilled and sophisticated actor."

Hafnium has in the past targeted US-based companies including infectious disease researchers, law firms, universities, defense contractors, think tanks and NGOs.

The potentially devastating hack is believed to have affected at least 30,000 Microsoft email servers in government and private networks and

has prompted calls for a firm response to state-sponsored attacks which could involve "hacking back" or other measures.

Microsoft in March released updates to fix the security flaws, which apply to on-premises versions of the software rather than cloud-based versions, and urged customers to apply them.

US Justice Department officials on Tuesday announced that, with backing from a court, they purged "malicious web shells" hackers had planted in hundreds of computers running Exchange Server software.

Web shells are bits of computer code that allow hackers to reach into computers remotely, and had been planted early this year by taking advantage of a weakness in Exchange, according to a Justice Department release.

"Today's operation removed one early hacking group's remaining web shells, which could have been used to maintain and escalate persistent, unauthorized access to US networks," Justice Department officials said.

Citation: Microsoft defends against new threat to Exchange (2021, April 14) retrieved 29 March 2023 from https://techxplore.com/news/2021-04-microsoft-defends-threat-exchange.html