

Forum:[Hack Forums](#)

Thread: [US nuclear weapons agency among 400 organisations breached by Chinese hackers](#)

MadScientist - July 26, 2025, 11:09 pm

US nuclear weapons agency 'among 400 organisations breached by Chinese hackers'

Microsoft says vulnerabilities in its SharePoint servers exposed as reports point to wave of attacks

Joanna Partridge

Wed 23 Jul 2025 10.39 EDT

Share

Microsoft says Chinese “threat actors”, including state-sponsored hackers, have exploited security vulnerabilities in its SharePoint document-sharing servers, with research indicating that several hundred government agencies and organisations have been breached.

Hackers have already breached 400 agencies, businesses and other groups, the Dutch cybersecurity company Eye Security said, adding: “We expect it may continue to rise as investigations progress.”

The majority of the victims are in the US, it found, while Bloomberg reported that the US agency charged with overseeing nuclear weapons, the National Nuclear Security Administration, was among the victims.

Microsoft said it had observed three groups – the Chinese state-backed Linen Typhoon and Violet Typhoon, and Storm-2603, which is believed to be China-based – using “newly disclosed security vulnerabilities” to target internet-facing servers hosting the platform.

Its announcement came amid reports in the Financial Times that Amazon was shutting down its artificial intelligence lab in Shanghai, while the consultancy McKinsey has stopped its China business from taking on work related to AI amid worsening geopolitical tensions between Washington and Beijing.

Microsoft and IBM have recently scaled back China-based research and development projects, as US officials are stepping up their scrutiny of US companies working in AI in China.

Microsoft said in a blogpost that the vulnerabilities were in on-premises SharePoint servers, which are commonly used by companies, rather than in its cloud-based service.

Many large organisations and businesses use SharePoint as a platform for storing documents and allowing colleagues to collaborate on them, and it is regarded as working well alongside other Microsoft products, including Office and Outlook.

Microsoft said the attacks had begun as early as 7 July and that the hackers were trying to exploit vulnerabilities to “gain initial access to target organisations”.

The vulnerabilities allow attackers to spoof authentication credentials and execute malicious code remotely on servers. Microsoft said it had observed attacks where the attackers had sent a request to a SharePoint server “enabling the theft of the key material”.

Microsoft said it had released security updates and advised all users of on-premises SharePoint systems to install them. It warned that it assessed with “high confidence” that the hacking groups would continue to attack unpatched on-premises SharePoint systems.

Source -

<https://www.theguardian.com/technology/2025/jul/23/sharepoint-targeted-by-chinese-threat-actor-hackers-says-microsoft>