The US Treasury Department was hacked

The US Treasury Department suffered a “major” security incident after a China state-sponsored hacker broke into the third-party remote management software it uses, as reported earlier by *The New York Times*.

In a letter to lawmakers seen by *The Verge*, the Treasury Department said BeyondTrust, the company behind its remote management software, notified the agency of a breach on December 8th.

The threat actor stole a key used by BeyondTrust “to secure a cloud-based service used to remotely provide technical support for Treasury Departmental Offices (DO) end users.” With the key, they overrode the security to remotely access those users’ workstations and “some unclassified documents” they maintained.

The Treasury Department said it worked with the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI following the attack, which has been attributed to a China state-sponsored Advanced Persistent Threat (APT) hacker. “The compromised BeyondTrust service has been taken offline and there is no evidence indicating the threat actor has continued access to Treasury systems or information,” US Treasury Department spokesperson Michael Gwin said in a statement to *The Verge*.

The attack seems to be linked to a security incident BeyondTrust disclosed earlier this month, impacting customers using its remote support software. At the time, BeyondTrust attributed the attack to a compromised API key for its remote

support software, adding that it “immediately revoked the API key, notified known impacted customers, and suspended those instances the same day.” *The Verge* reached out to BeyondTrust with a request for comment but didn’t immediately hear back.

“Treasury takes very seriously all threats against our systems, and the data it holds,” Gwin said. “Over the last four years, Treasury has significantly bolstered its cyber defense, and we will continue to work with both private and public sector partners to protect our financial system from threat actors.”

https://www.theverge.com/2024/12/30/24332429/us-treasury-department-beyondtrust-hack-security-breach