Chinese threat actors hacked NYC MTA using Pulse Secure zero-day

bleepingcomputer.com/news/security/chinese-threat-actors-hacked-nyc-mta-using-pulse-secure-zero-day/

Sergiu Gatlan

By
Sergiu Gatlan

- June 3, 2021
- 11:55 AM
- 0

Chinese-backed threat actors breached New York City's Metropolitan Transportation Authority (MTA) network in April using a Pulse Secure zero-day. Still, they failed to cause any data loss or gain access to systems controlling the transportation fleet.

According to Rafail Portnoy, MTA's Chief Technology Officer, while the attackers hacked into several MTA computer systems, they couldn't gain access to employee or customer information.

"The MTA quickly and aggressively responded to this attack, bringing on Mandiant, a leading cyber security firm, whose forensic audit found no evidence operational systems were impacted, no employee or customer information breached, no data loss and no changes to our vital systems," Portnoy said in a statement.

The third attack targeting MTA in recent years

MTA mitigated the vulnerability on April 21, one day after Pulse Secure issued an advisory, and CISA published an alert on the Pulse Secure zero-day exploited in the attack.

Additionally, existing security systems also hindered the attackers' attempts to move through the network.

"Importantly, the MTA's existing multi-layered security systems worked as designed, preventing spread of the attack and we continue to strengthen these comprehensive systems and remain vigilant as cyber-attacks are a growing global threat," Portnoy added.

The breach was the result of the third attack on the transportation authority's network in recent years, as MTA officials told the NY Times.

MTA is the largest North American transportation network serving more than 15.3 million people across a 5,000-square-mile travel area around New York City.

The transit authority operates multiple transportation agencies, including the MTA New York City Transit, MTA Bus, Long Island Rail Road, Metro-North Railroad, and MTA Bridges and Tunnels.

Dozens of US and European organizations also hacked

Cybersecurity firm FireEye revealed on April 20 that at least two Chinese-backed threat actors (tracked as UNC2630 and UNC2717) were actively exploiting a zero-day vulnerability to deploy 16 different malware families.

"Espionage activity by UNC2630 and UNC2717 supports key Chinese government priorities," FireEye said in a report published last month.

"Many compromised organizations operate in verticals and industries aligned with Beijing's strategic objectives outlined in China's recent 14th Five Year Plan."

The malware is custom-tailored for compromising Pulse Secure VPN appliances and used to maintain long-term access to networks, collect credentials, and steal proprietary data.

The zero-day was exploited together with other Pulse Secure bugs to hack the networks of dozens of US and European organizations across several verticals, including defense, government, high tech, transportation, and financial sectors.

A day later, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive ordering federal agencies to mitigate the security flaw within two days by disabling the Pulse Secure Collaboration and Windows File Share Browser features.

Pulse Secure issued security updates to address the zero-day bug on May 3 and also released the Pulse Connect Secure Integrity Tool that helps organizations check if hackers modified files on their Pulse Secure appliances.

CISA also updated mitigation measures shared in its alert and urges organizations to check the guidance published by Ivanti, Pulse Secure's parent company.

Related Articles:

GitHub: Attackers stole login details of 100K npm user accounts

Costa Rica declares national emergency after Conti ransomware attacks

US, EU blame Russia for cyberattack on satellite modems in Ukraine

Hackers display “blood is on your hands" on Russian TV, take down RuTube

NIST updates guidance for defending against supply-chain attacks