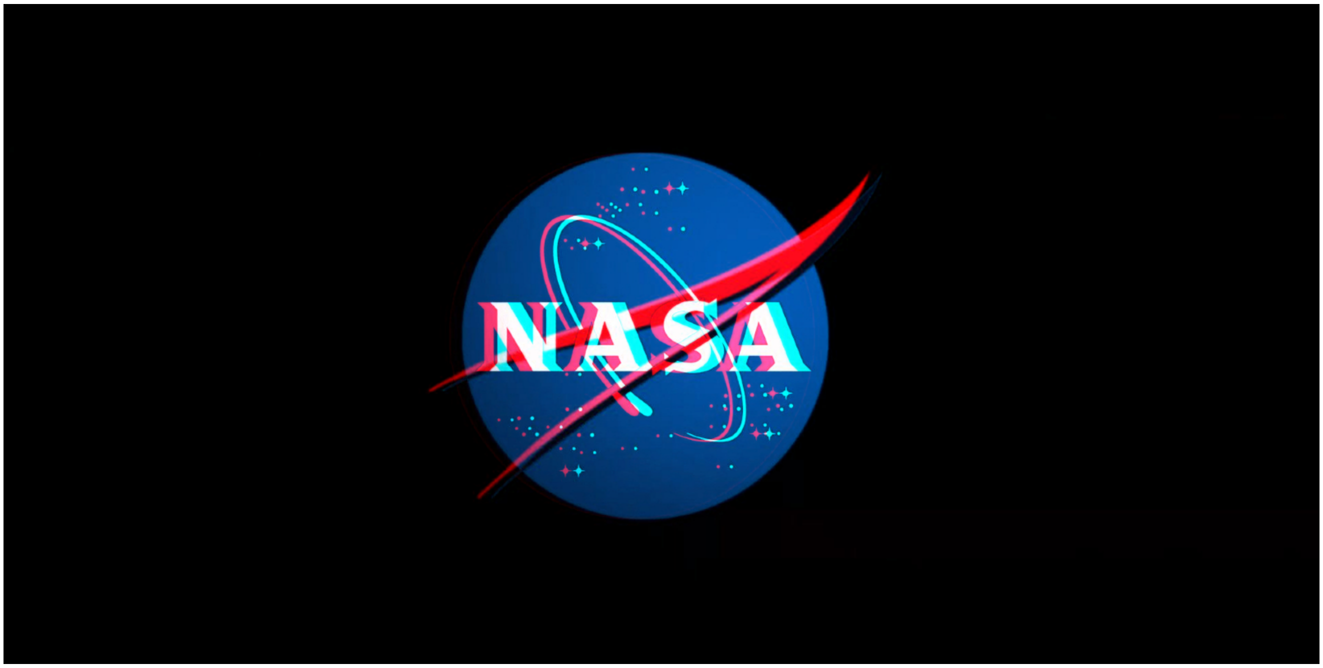
NASA and the FAA were also breached by the SolarWinds hackers

bleepingcomputer.com/news/security/nasa-and-the-faa-were-also-breached-by-the-solarwinds-hackers/

Sergiu Gatlan

By
Sergiu Gatlan

- February 24, 2021
- 08:32 AM
- 0



NASA and the US Federal Aviation Administration (FAA) have also been compromised by the nation-state hackers behind the SolarWinds supply-chain attack, according to a Washington Post report.

The two attacks are part of a broader espionage effort targeting and compromising multiple US government agencies over the last year.

NASA (short for National Aeronautics and Space Administration) is an independent U.S. federal agency coordinating its civilian space program. The FAA is the US civil aviation and international waters regulator.

NASA and FAA don't deny breach

While the US government has not publicly disclosed that NASA and the FAA were breached, the agencies' identities were confirmed by the Post with US officials after Anne Neuberger, White House’s deputy national security adviser, said that nine federal agencies were breached in the SolarWinds hack campaign.

A Transportation Department spokesperson said the agency is investigating the situation. A NASA spokeswoman added that the federal agency is working with CISA on "mitigation efforts to secure NASA’s data and network."

These two federal agencies are the last two to be identified after the hacks of seven others have already been acknowledged since the espionage campaign was uncovered.

The threat actor behind these attacks is currently tracked as StellarParticle (CrowdStrike), UNC2452 (FireEye), SolarStorm (Palo Alto Unit 42), and Dark Halo (Volexity).

While its identity is still anonymous, the FBI, CISA, ODNI, and the NSA issued a joint statement saying that it is likely a Russian-backed hacking group.

Microsoft shared a detailed timeline of the attacks& showing that the state hackers trojanized the company's Orion IT monitoring platform in February 2020 and later deployed a backdoor using the software's update mechanism on compromised networks in late-March.

Compromised federal agencies

The list of the seven other US government agencies confirmed as having been hit in the SolarWinds supply-chain attack includes:

- US& Department of the Treasury
- US& National Telecommunications and Information Administration (NTIA)
- US& Department of State
- The National Institutes of Health (NIH) (part of the US Department of Health)
- US& Department of Homeland Security (DHS)
- US& Department of Energy (DOE)
- US& National Nuclear Security Administration (NNSA)

In January, the Administrative Office of the US Courts disclosed an ongoing investigation following a potential compromise of the federal courts' case management and electronic case files system.

Last week, Microsoft also revealed that the SolarWinds hackers accessed and downloaded source code for a limited number of Azure, Intune, and Exchange components.

According to the Post's report, the Biden administration is also& planning to sanction Russia for the SolarWinds hacks and poisoning& opposition leader Alexei Navalny.

Related Articles:

FBI, CISA, and NSA warn of hackers increasingly targeting MSPs

FTC fines Twitter $150M for using 2FA info for targeted advertising

Hacker says hijacking libraries, stealing AWS keys was ethical research

Popular Python and PHP libraries hijacked to steal AWS keys

US Senate: Govt’s ransomware fight hindered by limited reporting