Autodesk reveals it was targeted by Russian SolarWinds hackers

bleepingcomputer.com/news/security/autodesk-reveals-it-was-targeted-by-russian-solarwinds-hackers/

Sergiu Gatlan

By
Sergiu Gatlan

- September 2, 2021
- 07:30 AM
- 0

Autodesk has confirmed that it was also targeted by the Russian state hackers behind the large-scale SolarWinds Orion supply-chain attack, almost nine months after discovering that one of its servers was backdoored with Sunburst malware.

The US software and services company provides millions of customers from the design, engineering, and construction sectors with CAD (computer-aided design), drafting, and 3D modeling tools.

"We identified a compromised SolarWinds server and promptly took steps to contain and remediate the incidents," Autodesk said in a recent 10-Q SEC filing.

"While we believe that no customer operations or Autodesk products were disrupted as a result of this attack, other, similar attacks could have a significant negative impact on our systems and operations."

An Autodesk spokesperson told BleepingComputer that the attackers did not deploy any other malware besides the Sunburst backdoor, likely because it was not selected for second stage exploitation or the threat actors didn't act quickly enough before they were detected.

"Autodesk identified a compromised SolarWinds server on December 13. Soon after, the server was isolated, logs were collected for forensic analysis, and the software patch was applied," the spokesperson said.

"Autodesk's Security team has concluded their investigation and observed no malicious activity beyond the initial software installation."

One of many tech companies breached in a large-scale hacking spree

The supply-chain attack that led to SolarWinds's infrastructure getting breached was coordinated by the hacking division of the Russian Foreign Intelligence Service (aka APT29, The Dukes, or Cozy Bear).

After gaining access to the company's internal systems, the attackers trojanized the Orion Software Platform source code and builds released between March 2020 and June 2020.

These malicious builds were later used to deliver a backdoor tracked as Sunburst to "fewer than 18,000," but, luckily, the threat actors only picked a substantially lower number of targets for second-stage exploitation.

As a direct result of this supply-chain attack, the Russian state hackers gained access to the networks of multiple US federal agencies and private tech sector firms.

Before the attack was disclosed, SolarWinds said it had 300,000 customers worldwide [1, 2], including over 425 US Fortune 500 companies, all top ten US telecom companies.

The company's customer list also included a long list of govt agencies (the US Military, the US Pentagon, the State Department, NASA, NSA, Postal Service, NOAA, the US Department of Justice, and the Office of the President of the United States).

At the end of July, the US Department of Justice was the latest US government entity to disclose that 27 US Attorneys' offices were breached during last year's SolarWinds global hacking spree.

SolarWinds has reported expenses of $3.5 million from dealing with last year's supply-chain attack in March 2021, including remediation and incident investigation costs.

Related Articles:

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

Google shut down caching servers at two Russian ISPs

Hacker says hijacking libraries, stealing AWS keys was ethical research

Popular Python and PHP libraries hijacked to steal AWS keys

Hackers target Russian govt with fake Windows updates pushing RATs

- APT29
- Autodesk
- Russia
- Russian SVR
- Security Breach
- SolarWinds
- Supply-Chain Attack

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: