SolarWinds patches critical Serv-U vulnerability exploited in the wild

bleepingcomputer.com/news/security/solarwinds-patches-critical-serv-u-vulnerability-exploited-in-the-wild/

Sergiu Gatlan

By
Sergiu Gatlan

- July 12, 2021
- 10:17 AM
- 0

SolarWinds is urging customers to patch a Serv-U remote code execution vulnerability exploited in the wild by "a single threat actor" in attacks targeting a limited number of customers.

"Microsoft has provided evidence of limited, targeted customer impact, though SolarWinds does not currently have an estimate of how many customers may be directly affected by the vulnerability," the company said in an advisory published on Friday.

"To the best of our understanding, no other SolarWinds products have been affected by this vulnerability. [..] SolarWinds is unaware of the identity of the potentially affected customers."

Only impacts servers with SSH enabled

The zero-day vulnerability (tracked as **CVE-2021-35211**) impacts Serv-U Managed File Transfer and Serv-U Secure FTP, and it enables remote threat actors to execute arbitrary code with privileges following successful exploitation.

According to SolarWinds, "if SSH is not enabled in the environment, the vulnerability does not exist."

The bug found by Microsoft Threat Intelligence Center (MSTIC) and Microsoft Offensive Security Research teams in the latest Serv-U 15.2.3 HF1 released in May 2021 also affects all prior versions.

SolarWinds has addressed the security vulnerability reported by Microsoft with the release of Serv-U version 15.2.3 hotfix (HF) 2.

Software Version	**Upgrade Paths**
Serv-U 15.2.3 HF1	Apply Serv-U 15.2.3 HF2, available in your Customer Portal
Serv-U 15.2.3	Apply Serv-U 15.2.3 HF1, then apply Serv-U 15.2.3 HF2, available in your Customer Portal
All Serv-U versions prior to 15.2.3	Upgrade to Serv-U 15.2.3, then apply Serv-U 15.2.3 HF1, then apply Serv-U 15.2.3 HF2, available in your Customer Portal

The company added that all other SolarWinds and N-able products (including the Orion Platform and Orion Platform modules) are unaffected by CVE-2021-35211.

"SolarWinds released a hotfix Friday, July 9, 2021, and **we recommend all customers using Serv-U install this fix immediately** for the protection of your environment," the US-based software firm warned.

SolarWinds provides additional info on how to find if your environment was compromised during the attacks Microsoft reported.

Customers can also request more information by opening a customer service ticket with the subject "Serv-U Assistance."

The SolarWinds Orion supply-chain attack

Last year, SolarWinds disclosed a supply-chain attack coordinated by the Russian Foreign Intelligence Service.

The attackers breached the company's internal systems and trojanized the Orion Software Platform source code and builds released between March 2020 and June 2020.

The 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.

Right before the attack was disclosed, SolarWinds' list of 300,000 customers worldwide [1, 2] included more than 425 US Fortune 500 companies, all top ten US telecom companies, and a long list of govt agencies, including 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.

Multiple US govt agencies confirmed that they were breached in the SolarWinds supply-chain attack, with the list including:

- the Department of the Treasury,
- the National Telecommunications and Information Administration (NTIA),
- the Department of State,
- the National Institutes of Health (NIH) (part of the U.S. Department of Health),
- the Department of Homeland Security (DHS),
- the Department of Energy (DOE),
- and the National Nuclear Security Administration (NNSA).

In March, SolarWinds reported expenses of $3.5 million from last year's supply-chain attack, including costs related to remediation and incident investigation.

Even though $3.5 million doesn't seem too much compared to the aftermath of the SolarWinds supply-chain attack, the incurred expenses reported so far were recorded only through December 2020, with high extra costs being expected throughout the subsequent financial periods.

Related Articles:

Zyxel fixes firewall flaws that could lead to hacked networks

F5 warns of critical BIG-IP RCE bug allowing device takeover

Synology warns of critical Netatalk bugs in multiple products

Access:7 vulnerabilities impact medical and IoT devices

QNAP warns users to disable AFP until it fixes critical bugs

- FTP
- RCE
- Remote Code Execution
- Serv-U
- SolarWinds

- Vulnerability
- Zero-Day

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: