Trustwave®

TRUSTWAVE SPIDERLABS FACT SHEET

SolarWinds Vulnerabilities

What Trustwave SpiderLabs Found

- Two security vulnerabilities in SolarWinds Orion Platform **(CVE-2021-25275** and **CVE-2021-25274)** and one vulnerability in SolarWinds Serv-U FTP for Windows **(CVE-2021-25276)**.
- All three vulnerabilities are severe bugs, with the most critical one in SolarWinds Orion Platform **(CVE-2021-25274)** allowing remote code execution with high privileges.
- To the best of Trustwave's knowledge, none of these identified vulnerabilities were exploited in the recent SolarWinds attacks or in any attacks "in the wild".
- Trustwave reported all three findings to SolarWinds and patches were released in a very timely manner.
- Full details can be found in our vulnerability blog post.

Why It's Important

- SolarWinds Orion Platform **(CVE-2021-25275)**: SolarWinds credentials are stored in an insecure manner that could allow any local users, despite privileges, to take complete control over the SOLARWINDS_ORION database. From here, one can steal information or add a new admin-level user to be used inside SolarWinds Orion products.
- SolarWinds Orion Platform **(CVE-2021-25274)**: Improper use of Microsoft Messaging Queue (MSMQ) could allow any remote unprivileged user the ability to execute any arbitrary code in the highest privilege.
- SolarWinds Serv-U FTP for Windows **(CVE-2021-25276)**: Any local user, regardless of privilege, can create a file that can define a new Serv-U FTP admin account with full access to the C:\ drive. This account can then be used to log in via FTP and read or replace any file on the drive.

Immediate Recommended Protections

- SolarWinds credentials are stored in an insecure manner that could allow any local users, despite privileges, to take complete control over the SOLARWINDS_ORION database. From here, one can steal information or add a new admin-level user to be used inside SolarWinds Orion products.
  - › Orion Platform 2020.2.4
  - › ServU-FTP 15.2.2 Hotfix 1

Planned Future Updates from Trustwave SpiderLabs

- We have purposely left out specific Proof of Concept (PoC) code in the full blog post in order to give SolarWinds users longer to patch. A blog update with PoC code will go live on Feb. 9.
- PoC code helps information security professionals better understand these issues and can help them develop protections or test for vulnerable systems in ways specific to their environment.

Trustwave Product Protections

- Trustwave vulnerability scanning products can detect these vulnerabilities and Trustwave IDS/IPS products include signatures that can detect network exploitation of **CVE-2021-25274**.