CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-008

Critical Vulnerabilities in SolarWinds Orion Platform

February 4, 2021 — v1.0

TLP:WHITE

Summary

Three critical vulnerabilities have been found in **SolarWinds Orion** platform. Two of them could be exploitable by a local attacker and a third one, the most severe of all, allows a remote, unprivileged actor to take control of the platform [1, 2]. These vulnerabilities are separate and not directly related to the earlier reported Sunburst attack.

Technical Details

The vulnerabilities were assigned **CVE-2021-25274** [3], **CVE-2021-25275** [4], and **CVE-2021-25276** [5].

CVE-2021-25274

Analysing a demo copy of the **SolarWinds Orion** software, the researcher from Trustwave [2] noticed that it uses the Microsoft Message Queue (MSMQ). He noticed that the **SolarWinds Orion Collector** service relies heavily on MSMQ, with a large list of private queues available, all of them unauthenticated. This means that unauthenticated users can send messages to the queues over TCP port 1801. Due to an insecure deserialisation, an unprivileged user can execute arbitrary code remotely.

SolarWinds addressed this issue by adding a digital signature validation step when new messages arrive. Without a valid signature, messages are no longer processed. MSMQ, though, remains unauthenticated and can receive messages from anyone.

CVE-2021-25275

The second vulnerability discovered was that the credentials for the **Orion** backend database were insufficiently protected and local users had unrestricted access to them. The researcher found the sensitive data in the `SOLARWINDS_ORION` configuration file that could be read by locally authenticated users. With only one line of code, the researcher decrypted the credentials.

After authenticating to the Microsoft SQL Server with the recovered credentials, a threat actor would have complete control over the **SolarWinds Orion** database and could steal information or add admin-level users.

CVE-2021-25276

The third vulnerability is in the **SolarWinds Serv-U FTP Server**. The researcher discovered that the accounts are stored in separate files on the disk and that an authenticated user has access to them. The FTP server runs with LocalSystem permissions, so by creating an admin account, an attacker could set the home directory to the root of the system drive and thus open the door to read or replace any file there.

Affected Products

- SolarWinds Orion Platform

Recommendations

SolarWinds released patches that address the vulnerabilities described in this advisory.

CERT-EU recommends installing **Orion Platform 2020.2.4** [6] and applying **Hotfix 1 for ServU-FTP 15.2.2** [7].

References

[1] https://www.bleepingcomputer.com/news/security/solarwinds-patches-critical-vulnerabilities-in-the-orion-platform/

[2] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/full-system-control-with-new-solarwinds-orion-based-and-serv-u-ftp-vulnerabilities/

[3] https://nvd.nist.gov/vuln/detail/CVE-2021-25274

[4] https://nvd.nist.gov/vuln/detail/CVE-2021-25275

[5] https://nvd.nist.gov/vuln/detail/CVE-2021-25276

[6] https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/release_notes/orion_platform_2020-2-4_release_notes.htm

[7] https://downloads.solarwinds.com/solarwinds/Release/HotFix/Serv-U-15.2.2-Hotfix-1.zip