Security Advisory 2024-055

SolarWinds High-Severity Vulnerabilities

June 8, 2024 — v1.0

TLP:CLEAR

History:

- *08/06/2024 — v1.0 – Initial publication*

Summary

On the 4th and 5th of June 2024, SolarWinds published four separate security advisories related to high-severity vulnerabilities in multiple products [1]. CERT-EU strongly recommends patching them as soon as possible.

Technical Details

CVE-2024-28995 - SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive files on the host machine [2].

CVE-2024-28996 - The SolarWinds Platform was determined to be affected by a SWQL Injection Vulnerability. Attack complexity is high for this vulnerability [3].

CVE-2024-28999 - The SolarWinds Platform was determined to be affected by a Race Condition Vulnerability affecting the web console [4].

CVE-2024-29004 - The SolarWinds Platform was determined to be affected by a stored cross-site scripting vulnerability affecting the web console. High-privileged user credentials are needed, and user interaction is required to exploit this vulnerability [5].

Affected Products

- SolarWinds Serv-U 15.4.2 HF 1 and previous versions (CVE-2024-28995)
- SolarWinds Platform 2024.1 SR 1 and previous versions (CVE-2024-28996, CVE-2024-28999, and CVE-2024-29004)

Recommendations

SolarWinds has released updated versions of their products where these vulnerabilities are patched. CERT-EU strongly recommends updating the relevant products as soon as possible.

References

[1] https://www.solarwinds.com/trust-center/security-advisories

[2] https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28995

[3] https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28996

[4] https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28999

[5] https://www.solarwinds.com/trust-center/security-advisories/cve-2024-29004