



## ADV2026\_111 SolarWinds Security Advisory (February 25<sup>th</sup>, 2026)

SolarWinds published a security advisory highlighting vulnerabilities in the following product on February 24<sup>th</sup>, 2026. It is recommended that you take the necessary precautions by ensuring your product is always updated.

- SolarWinds Serv-U - versions prior to 15.5.4

For more information on this update, you can follow these URL:

- [SolarWinds Serv-U Broken Access Control Remote Code Execution Vulnerability \(CVE-2025-40538\)](#)
- [SolarWinds Security Vulnerabilities](#)

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

### References

- SolarWinds Serv-U Broken Access Control Remote Code Execution Vulnerability (CVE-2025-40538). (n.b.). Retrieved from SolarWinds. <https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40538>
- SolarWinds Security Vulnerabilities. (n.b.). Retrieved from SolarWinds. <https://www.solarwinds.com/trust-center/security-advisories>
- SolarWinds security advisory. (February 24, 2026). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/solarwinds-security-advisory-av26-165>