

Department of the Environment, Climate & Communications



NCSC Alert

Critical Vulnerability exists in SolarWinds Serv-U (CVE-2024-28995, CVSSv3: 7.5)

Thursday 18th July, 2024

STATUS: TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP-CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP-CLEAR** information may be shared without restriction.*

For more information on the Traffic Light Protocol, see <https://www.first.org/tp/>.

Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-06-06T09:15:00

Vendor: SolarWinds

Product: SolarWinds Serv-U

CVE ID: CVE-2024-28995

CVSS3.0 Score¹: 7.5

EPSS²: 0.995040000

Summary: SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive files on the host machine.

More information related to this issue can be found at the following link:

- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28995>

Products Affected

- SolarWinds SolarWinds Serv-U

Impact

Common Weakness Enumeration (CWE)³: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Present in CISA Known Exploited Vulnerability(KEV)⁴ catalog: YES

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from SolarWinds .

Additional recommendations and mitigations for CVE-2024-28995 can be found in the respective link below:

- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28995>

¹<https://www.first.org/cvss/v3.0/specification-document>

²https://www.first.org/epss/articles/prob_percentile_bins

³<https://cwe.mitre.org/>

⁴<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: [ncsc_gov_ie](https://twitter.com/ncsc_gov_ie)
LinkedIn: [ncsc-ie](https://www.linkedin.com/company/ncsc-ie)



**An Láirionad Náisiúnta
Cibearshlándála
National Cyber Security Centre**