BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

June 11, 2024

Vulnerability in SolarWinds Serv-U Could Allow for Path Transversal

OVERVIEW

A vulnerability in SolarWinds Serv-U could allow for path transversal, leading to disclosure of sensitive information. SolarWinds Serv-U is a managed file transfer solution, hosted on Windows and Linux-based servers, used to store and share files across an enterprise network. Exploitation of this vulnerability could allow for the disclosure of files and directories on the host. Depending on the permissions associated with the files, an attacker could view content within them. Files with stricter access controls and file permissions could be less impacted.

THREAT INTELLIGENCE

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED

- SolarWinds Serv-U versions prior to 15.4.2 HF 2

RECOMMENDATIONS

We recommend the following actions be taken:

- Apply appropriate updates provided by SolarWinds to vulnerable systems immediately after appropriate testing.
- Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.
- Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.
- Use intrusion detection signatures to block traffic at network boundaries.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.

REFERENCES

- https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28995
- https://www.helpnetsecurity.com/2024/06/07/cve-2024-28995/
- https://nvd.nist.gov/vuln/detail/CVE-2024-28995