BLACKSWAN CYBERSECURITY

THREAT ADVISORY

June 26, 2024

SolarWinds Ser-U File Transfer Flaw being Exploited

Summary

A high-severity flaw in SolarWinds Serv-U file transfer software (CVE-2024-28995) is being actively exploited. This is a directory traversal vulnerability that allows attackers to read sensitive files on the host machine.

CVE-ID	CVSSv3 Score
CVE-2024-28995	8.6

Threat intelligence

- Exploitation attempts have been seen in the wild
- Exploit is trivial
- Proof of Concept is publicly available

Vulnerability Details

The vulnerability is a directory traversal bug affecting all versions of Serv-U software, allowing unauthenticated attackers to read any arbitrary file on the host machine, if they know the file path and the file is not locked.

Rapid7 described the flaw as trivial to exploit, enabling external attackers to access critical files on the host. This vulnerability could be used in "smash-and-grab" attacks where adversaries quickly exfiltrate data from file transfer solutions to extort victims.

Exploits of this vulnerability have been actively observed in the wild, with attempts recorded from China to access files like /etc/passwd. Additionally, GreyNoise reported opportunistic attacks using the flaw against its honeypot servers. Contrast Security researchers noted that successful exploitation could lead to further attacks by chaining the vulnerability to access credentials and system files, potentially compromising other systems and applications.

Affected Products

All versions of the software prior to and including:

- Serv-U 15.4.2 HF 1
- Serv-U FTP Server 15.4
- Serv-U Gateway 15.4
- Serv-U MFT Server 15.4
- Serv-U File Server 15.4

Solution

- Serv-U version 15.4.2 HF 2 (15.4.2.157)

Recommendations

- Update to Serv-U version 15.4.2 HF 2 (15.4.2.157) immediately.
- Monitor network traffic for unusual activity indicative of exploitation attempts.
- Restrict access to sensitive files and directories.
- Implement strong access controls and authentication mechanisms.
- Use intrusion detection systems to detect and respond to potential attacks.
- Conduct regular security audits and vulnerability assessments on all systems.
- Ensure all security tools and defenses are up-to-date and properly configured.

References

- https://thehackernews.com/2024/06/chinese-hackers-deploy-spicerat-and.html
- https://github.com/bigb0x/CVE-2024-28995
- https://attackerkb.com/topics/2k7UrkHyl3/cve-2024-28995/rapid7-analysis
- https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28995