

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Active Exploitation of SolarWinds Serv-U Flaw for Accessing Private Data

Date of Publication

June 21, 2024

Admiralty Code

A1

TA Number

TA2024238




Summary

First Seen: June 2024

Affected Products: SolarWinds Serv-U

Impact: Threat actors are actively exploiting a critical path-traversal vulnerability, CVE-2024-28995, in SolarWinds Serv-U. By leveraging publicly available proof-of-concept (PoC) exploits, attackers can successfully exploit this vulnerability, allowing unauthenticated access to read sensitive files on the target server.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-28995	SolarWinds Serv-U Directory Transversal Vulnerability	SolarWinds Serv-U			

Vulnerability Details

#1

SolarWinds has announced a serious security issue, CVE-2024-28995, affecting their Serv-U file transfer server, available in two versions: Serv-U FTP and Serv-U MFT. This high-severity directory traversal vulnerability can be exploited by attackers to read sensitive files on the target server without needing to log in.

#2

Cybercriminals are already taking advantage of this flaw, using publicly available proof-of-concept (PoC) exploits to carry out directory traversal attacks. This vulnerability arises from a problem in how the server handles certain input sequences, allowing remote attackers to send specially crafted requests to access arbitrary files on the system.

#3

Honeypots mimicking vulnerable Serv-U systems have indicated both manual and automated attack strategies targeting the flaw, confirming an active and ongoing threat and emphasizing the importance of implementing immediate security measures.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28995	SolarWinds Serv-U 15.4.2 HF 1 and previous versions	cpe:2.3:a:solarwinds:serv-u:*:*:*:*:*:* cpe:2.3:a:solarwinds:serv-u:15.4.2:-:*:*:*:*:* cpe:2.3:a:solarwinds:serv-u:15.4.2:hotfix1:*:*:*:*:*	CWE-22

Recommendations



Update: To mitigate this risk, SolarWinds has released version the 15.4.2 Hotfix 2 to address the CVE-2024-28995 vulnerability. It is crucial for SolarWinds Serv-U users to promptly update to this version to protect their systems from potential exploitation.



Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0005 Defense Evasion	TA0009 Collection	TA0010 Exfiltration
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1005 Data from Local System	T1006 Direct Volume Access

Patch Details

To address the vulnerability (CVE-2024-28995), SolarWinds has published version 15.4.2 Hotfix 2. It is strongly recommended that users update to this version immediately to protect their systems from potential exploitation.

Links:

<https://support.solarwinds.com/SuccessCenter/s/article/Serv-U-15-4-2-Hotfix-2-Release-Notes>

References

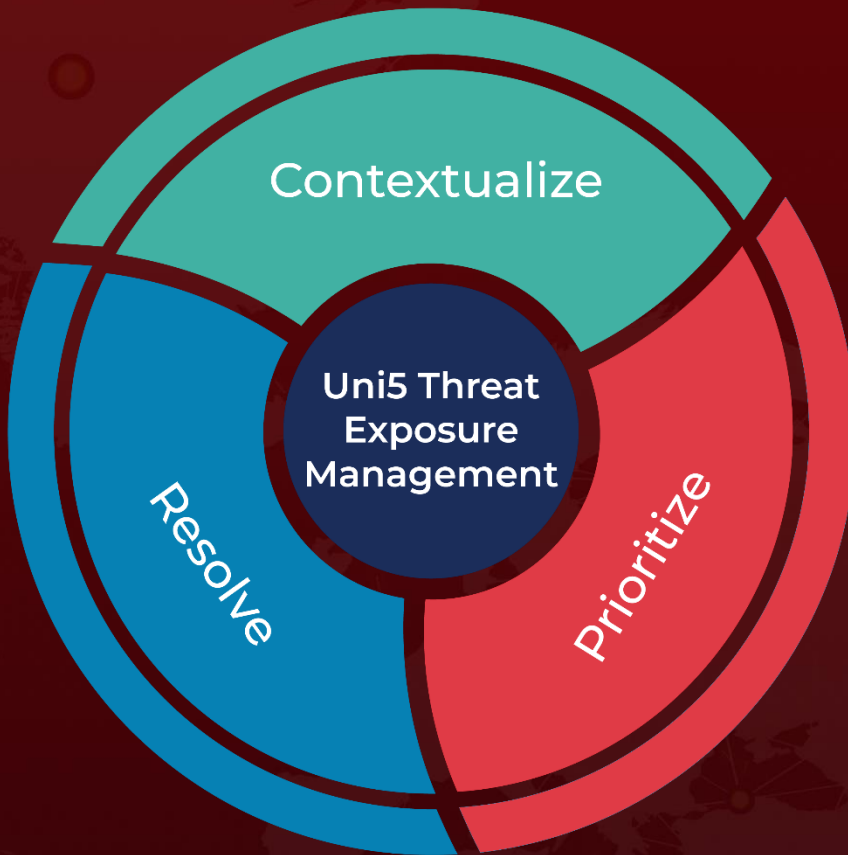
<https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28995>

<https://github.com/bigb0x/CVE-2024-28995/blob/main/CVE-2024-28995.py>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

June 21, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com