



# WÜRTH PHOENIX

**BUSINESS SOFTWARE - IT MANAGEMENT – PROCESS CONSULTING – CYBER SECURITY**

## **SolarWinds Serv-U Directory Traversal Vulnerability**

**June 2024**

---

SOC Informative Report

---

## Document details

### **Title of the activity**

SolarWinds Serv-U Directory Traversal Vulnerability

### **Summary**

Report containing information regarding the vulnerability CVE-2024-28995

### **Target audience**

SOC and SOC AdS representatives

### **Confidentiality level (Clear/Green/Amber/Amber+Strict/Red)**

CLEAR

### **Publication date**

19/06/2024

### **Written by**

Mirko Ioris, Luca Zeni

### **Reviewed by**

Massimo Giaimo

## Confidentiality level

A level of confidentiality is applied to the document, marked by the "Confidentiality Level" item on the front page. The values that can be used (RED / AMBER / AMBER+STRICT / GREEN / CLEAR) have the following meanings:

**TLP:RED** = Reserved for participants only.

Sources may use TLP:RED when the information cannot be effectively used by other parties and could impact a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with parties outside the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most cases, TLP:RED should be exchanged verbally or in person.

**TLP:AMBER** = Limited disclosure, restricted to participants' organizations.

**TLP:AMBER+STRICT** limits sharing to the *organization* only.

Sources may use TLP:AMBER when the information requires support to act effectively but poses risks to privacy, reputation, or operations if shared outside the organizations involved. Recipients may share TLP:AMBER information only with members of their own organization and with clients or customers who need to know the information to protect themselves or prevent further harm.

Note: If the source wishes to limit sharing **only** to the organization, it must specify TLP:AMBER+STRICT.

**TLP:GREEN** = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when the information is useful for the awareness of all participating organizations, as well as with colleagues within the community or broader sector. Recipients may share TLP:GREEN information with colleagues and partner organizations within their sector or community, but not through publicly accessible channels. Information in this category may be widely disseminated within a particular community. TLP:GREEN information may not be released outside the community.

---

**TLP:CLEAR** = Disclosure is not limited.

Sources may use TLP:CLEAR when the information poses little or foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

---

# Table of contents

<b>SolarWinds Serv-U Directory Traversal Vulnerability</b>	<b>0</b>
<b>Document details</b>	<b>1</b>
<b>Confidentiality level</b>	<b>2</b>
<b>Table of contents</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>Vulnerability Overview</b>	<b>5</b>
<b>Attack surface</b>	<b>6</b>
<b>PoC and IOC</b>	<b>9</b>
<b>Affected products</b>	<b>10</b>
<b>Remediation</b>	<b>10</b>
Step by step guide	10
<b>Bibliography</b>	<b>11</b>

## Introduction

A security researcher called **Hussein Daher** discovered a security vulnerability in SolarWinds Serv-U file transfer server. **Solarwinds** security, product, and engineering teams worked together with the researcher to fix the vulnerability.

On June 5, 2024, Solarwinds disclosed the vulnerability [1]. It was classified as **Directory Traversal** and was assigned the CVE number **CVE-2024-28995**. A hotfix suitable for both Windows and Linux was released the same day [2].

## Vulnerability Overview

This directory traversal vulnerability is extremely easy to exploit by a remote user. By simply sending a modified HTTP request, an **unauthenticated attacker** can retrieve the contents of any file on the vulnerable server to which the Serv-U service account has access permissions.

Two different CVSS values were assigned to the vulnerability:


- SolarWinds - **8.6** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)
- NIST - **7.5** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)


The main difference lies in the **Scope**, evaluated as changed by SolarWinds and unchanged by NIST.

CVE Number	CVSS Score	EPSS Score
CVE-2024-28995 [3]	7.5 (High) 8.6 (High)	0.11% (Low)

# Attack surface

We scanned the network in search of vulnerable internet-exposed devices. We used different device search engines and the results are shared here below:

Shodan Query (19/06/2024)	
product:"Serv-U ftpd"	
	

FOFA Query (19/06/2024)																																				
app="SolarWinds-Serv-U-FTP"																																				
190,267 results ( 128,716 unique IP ) , 2013 ms																																				
(results refer to devices seen in the last year)																																				
<h3>TOP COUNTRIES/REGIONS</h3> <table><tbody><tr><td>&gt;&gt; China</td><td></td><td>105,212</td></tr><tr><td>&gt;&gt; United States</td><td></td><td>40,115</td></tr><tr><td>&gt;&gt; Taiwan, P.R.C.</td><td></td><td>13,660</td></tr><tr><td>&gt;&gt; Hong Kong</td><td></td><td>6,439</td></tr><tr><td>&gt;&gt; Germany</td><td></td><td>3,062</td></tr></tbody></table> 	>> China		105,212	>> United States		40,115	>> Taiwan, P.R.C.		13,660	>> Hong Kong		6,439	>> Germany		3,062	<h3>TOP OPEN PORTS</h3> <table><tbody><tr><td>21</td><td>133,157</td></tr><tr><td>443</td><td>11,526</td></tr><tr><td>80</td><td>5,834</td></tr><tr><td>2121</td><td>3,279</td></tr><tr><td>990</td><td>3,032</td></tr></tbody></table> <h3>TOP SERVERS</h3> <table><tbody><tr><td>Serv-U/15.1.6.25</td><td>4,432</td></tr><tr><td>Serv-U/15.1.7.162</td><td>3,052</td></tr><tr><td>Serv-U/15.0.1.20</td><td>1,692</td></tr><tr><td>Serv-U</td><td>1,672</td></tr><tr><td>Serv-U/15.1.2.189</td><td>1,219</td></tr></tbody></table>	21	133,157	443	11,526	80	5,834	2121	3,279	990	3,032	Serv-U/15.1.6.25	4,432	Serv-U/15.1.7.162	3,052	Serv-U/15.0.1.20	1,692	Serv-U	1,672	Serv-U/15.1.2.189	1,219
>> China		105,212																																		
>> United States		40,115																																		
>> Taiwan, P.R.C.		13,660																																		
>> Hong Kong		6,439																																		
>> Germany		3,062																																		
21	133,157																																			
443	11,526																																			
80	5,834																																			
2121	3,279																																			
990	3,032																																			
Serv-U/15.1.6.25	4,432																																			
Serv-U/15.1.7.162	3,052																																			
Serv-U/15.0.1.20	1,692																																			
Serv-U	1,672																																			
Serv-U/15.1.2.189	1,219																																			



### Hunter Query (19/06/2024)

protocol.banner="Serv-U FTP"

Results 70.680      Filter: **Past week** ▼

Results 133.031      Filter: **Past month** ▼

Results 331.962      Filter: **Past year** ▼

**Statistics**

Total IP Count	43.8K
Internet Services	133K

**Filter Mode**

**By Location**

- ▶ **China**
103.8K
- ▶ **United States**
20.9K
- ▶ **Australia**
1.9K
- ▶ **Russia**
839
- ▶ **Germany**
470

**Statistics**

Total IP Count	31.9K
Internet Services	70.7K

**Filter Mode**

**By Location**

- ▶ **China**
50.3K
- ▶ **United States**
14.6K
- ▶ **Australia**
1.4K
- ▶ **Russia**
570
- ▶ **United Kingdom**
337

Focus on last month

Focus on last week

---

It is important to note that not all exposed devices reported in the above queries may be vulnerable.

## PoC and IOC

On June 15th user **bigb0x** published a PoC of the exploit on GitHub [4].

Security experts at **GreyNoise** [5] deployed two copies of an experimental honeypot to emulate a real vulnerable application and monitor incoming exploit attempts.

Here is a list of IOCs observed committing different exploit attempts:

(last update 19 June)

185.196.10.2

221.4.215.215

120.245.64.189

## Affected products

The affected product are:

- **SolarWinds Serv-U 15.4.2 HF 1 and earlier version**

## Remediation

The **Solarwinds** security team has already published a hotfix to prevent exploits of CVE-2024-28995, available for all the compromised product and version.

- **SolarWinds Serv-U 15.4.2 HF 2 and later are patched**

## Step by step guide

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

---

## Bibliography

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

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

[3]<https://nvd.nist.gov/vuln/detail/cve-2024-28995>

[4] <https://github.com/bigb0x/CVE-2024-28995>

[5]<https://www.labs.greynoise.io/grimoire/2024-06-solarwinds-serv-u/>