Path traversal in SolarWinds Serv-U File Server <=15.2.1

From: Jack Misiura via Fulldisclosure <fulldisclosure () seclists org>
Date: Mon, 8 Feb 2021 05:50:27 +0000

```
Title: Path traversal


Product: SolarWinds Serv-U FTP Server


Vendor Homepage: https://www.solarwinds.com/


Vulnerable Version: 15.2.1 and lower


Fixed Version: 15.2.2


CVE Number: CVE-2020-27994


Author: Jack Misiura from The Missing Link


Website: https://www.themissinglink.com.au


Timeline:


2020-10-28 Disclosed to Vendor

2021-01-21 Vendor releases patched version

2021-08-02 Publication


1. Vulnerability Description


SolarWinds Serv-U File Server through 15.2.1 does not correctly validate path information, allowing the disclosure of
files and directories outside of the user's home directory via a specially crafted GET request.



2. PoC


On a vulnerable Serv-U installation issue the following GET request to get a listing of files and directories above
the
user's directory:


https://<serv-u host>/Web Client/?Command=List&dir=\..\*.*


The user *MUST* be locked to their directory, and only access granted must be the said directory. Directory listing
must be enabled. If any of the above is not present, the exploit will not work.


3. Solution


The vendor provides an updated version (15.2.2) which should be installed immediately.


4. Advisory URL


https://www.themissinglink.com.au/security-advisories




Jack Misiura


Application Security Consultant


a


9-11 Dickson Avenue


Artarmon
```

NSW

2064

p

1300 865 865

os

+61 2 8436 8585

w

<https://www.themissinglink.com.au/> themissinglink.com.au

<https://www.linkedin.com/company/the-missing-link-pty-ltd/>

<https://www.facebook.com/The-Missing-Link-268395013346228/?ref=bookmarks>

<https://twitter.com/TML_au>

<https://www.youtube.com/channel/UC2kd4mDmBs3SjW4lX3fFHnQ>

<https://www.instagram.com/the_missing_link_it/>

<https://www.themissinglink.com.au/our-inclusive-culture>

Attachment: smime.p7s
Description:

By Date By Thread

Current thread:

Path traversal in SolarWinds Serv-U File Server <=15.2.1 ***Jack Misiura via Fulldisclosure (Feb 11)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License