



[Full Disclosure](#) mailing list archives

[By Date](#) [By Thread](#)



Stored XSS in SolarWinds Serv-U File Server <=15.2.1

From: Jack Misiura via FullDisclosure <fulldisclosure () seclists.org>

Date: Mon, 8 Feb 2021 05:51:11 +0000

Title: Stored XSS

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-2020-28001

Author: Jack Misiura from The Missing Link

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

Timeline:

2020-10-30 Disclosed to Vendor

2021-01-21 Vendor releases patched version

2021-08-02 Publication

1. Vulnerability Description

SolarWinds Serv-U FTP server through 15.2.1 does not correctly sanitize and validate the user-supplied directory names, allowing malicious users to create directories that when clicked on (in the breadcrumb menu) will trigger XSS payloads.

2. PoC

On a vulnerable Serv-U FTP server installation, create a directory named as such:

```
%27%29%3Ba%3Dfunction%28b%29%20%7B%20alert%28%22XSS%22%29%3B%20%7D%3Ba%28%27
```

The payload contains ');a=function(b) { alert("XSS"); };a('

As soon as a user clicks on the directory name in the breadcrumb menu, it will trigger the stored XSS.

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/UC2kd4mDmBs3SiW4lX3FFHnQ>

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

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

CAUTION - This message may contain privileged and confidential information intended only for the use of the addressee named above. If you are not the intended recipient of this message you are hereby notified that any use, dissemination, distribution or reproduction of this message is prohibited. If you have received this message in error please notify The Missing Link immediately. Any views expressed in this message are those of the individual sender and may not necessarily reflect the views of The Missing Link.



Attachment: [amime.p7s](#)

Description:

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[By Date](#) [By Thread](#)

Current thread:

Stored XSS 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](#)

