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/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:

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

Site Search