

Search
)

Home Files News About Contact &[SERVICES_TAB] Add New

SolarWinds Serv-U FTP Server 15.2.1 Cross Site Scripting

Authored by Jack Misiura

Posted Feb 12, 2021

SolarWinds Serv-U FTP Server versions through 15.2.1 do 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 cross site scripting payloads.

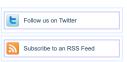
tags | exploit, xss advisories | CVE-2020-28001 | SHA-256 | 63b2c20217bc49cd26d5d1117a3e0ef300ddd3efe77e545937de5ae02474c7ac | Download | Favorite | View

Share This

Like

LinkedIn Reddit Digg StumbleUpon

Change Mirror Download
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:
\$2742943Ba43Dfunction\$28b42942047B82Oalert\$28\$22XSS\$2242943B\$2047D\$3Ba828827
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
9-11 Dickson Avenue
Artarmon
NSW
2064



Su	Мо	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

31	
Тор	Authors In Last 30 Days
Red H	at 150 files
Ubunt	tu 68 files
Liquio	Worm 23 files
Debia	n 16 files
malvu	In 11 files
nu11s	ecur1ty 11 files
Gento	O 9 files
Goog	le Security Research 6 files
Julien	Ahrens 4 files
T. Wel	ber 4 files

File Tags	File Archives
ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	Systems
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

p	Spoof (2,166)	SUSE (1,444)
	SQL Injection (16,102)	Ubuntu (8,199)
1300 865 865	TCP (2,379)	UNIX (9,159)
	Trojan (686)	UnixWare (185)
OS .	UDP (876)	Windows (6,511)
+61 2 8436 8585	Virus (662)	Other
	Vulnerability (31,136)	Otrici
w	Web (9,365)	
w .	Whitepaper (3,729)	
<https: www.themissinglink.com.au=""></https:> themissinglink.com.au		
	X86 (946) XSS (17,494)	
	Other	
<https: company="" the-missing-link-pty-ltd="" www.linkedin.com=""></https:>		
https://www.facebook.com/The-Missing-Link-268395013346228/?ref=bookmarks>		
<https: au="" tml="" twitter.com=""></https:>		
<pre><https: channel="" uc2kd4mdmbs3sjw41x3ffhnq="" www.youtube.com=""></https:></pre>		
<pre><https: it="" link="" missing="" the="" www.instagram.com=""></https:></pre>		
<https: our-inclusive-culture="" www.themissinglink.com.au=""></https:>		
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.		

Login or Register to add favorites



Site Links About Us Hosting By Follow us on Twitter News by Month History & Purpose Rokasec News Tags Contact Information Subscribe to an RSS Feed Files by Month Terms of Service File Tags File Directory Privacy Statement

Copyright Information