SolarWinds Serv-U FTP Server 15.2.1 Path Traversal

Authored by Jack Misiura | Posted Feb 12, 2021

SolarWinds Serv-U File Server versions through 15.2.1 do 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.

tags | exploit, file inclusion
advisories | CVE-2020-27994
SHA-256 | 64b515c78c524df69e596a9ac43e62c6feeaae73ff31f506f5da5c63c7573d1a Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	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

Top Authors In Last 30 Days

- Red Hat 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

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/UC2kd4mDmBs3SjW41X3fFHnQ>

<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.

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Login or Register to add favorites

packet storm
© 2022 Packet Storm. All rights reserved.

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed