Windows "Users" Directory Weak ACLs Vulnerability (CVE-2021-25276)

Summary

In SolarWinds Serv-U before 15.2.2 Hotfix 1, there is a directory containing user profile files (that include users' password hashes) that is world readable and writable. An unprivileged Windows user (having access to the server's filesystem) can add an FTP user by copying a valid profile file to this directory. For example, if this profile sets up a user with a C:\ home directory, then the attacker obtains access to read or replace arbitrary files with LocalSystem privileges.

Affected Products

- Serv-U versions 15.2.2 and earlier

Fixed Software Release

- Serv-U 15.2.2 HF 1

Acknowledgments

- Martin Rakhmanov, Trustwave

Advisory Details

Severity

8.8 High

Advisory ID

CVE-2021-25276

First Published

01/18/2021

Last Updated

02/04/2021

Version

Serv-U 15.2.2 HF 1

CVSS Score

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H