U UNISPHERE SOLUTIONS

✉ info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00172

## MICROSOFT DISCOVERS SOLARWINDS VULNERABILITY

DATE ISSUED: 19th July 2021

| | | | |
|---|---|---|---|
| IMPACT | LOW | [✓ MEDIUM] | HIGH |
| EASE OF EXPLOIT | [✓ HARD] | MEDIUM | EASY |

## OVERVIEW

A further hot-fix has been has been released by SolarWinds after Microsoft discovered more vulnerabilities in the SolarWinds Serv-U Managed File Transfer and Secure FTP products which has been exploited in a limited number of customers.

## BREAKDOWN

This further Remote Code Execution (RCE) vulnerability was discovered by Microsoft researchers and a Proof of Concept (PoC) provided to SolarWinds who have responded by releasing a temporary fix and allows an attacker to run arbitrary code under privilege. A "limited" selection of customer have been targeted by a threat actor who has successfully exploited the vulnerability, and at this stage looks like a lone threat actor. This current attack is observed to be outside of the supply-chain attacks earlier this year as a stand-alone vulnerability.

## REMEDIATION STEPS

- All customers using Serv-U version 15.2.3 HF1 (released in May 2021) should upgrade to the latest version.
- Apply all hot fixes provided by SolarWinds.
- Subscribe to the RSS Feed for further updates.

## REFERENCES & RESOURCES

| | |
|---|---|
| Threatpost | https://threatpost.com/solarwinds-hotfix-zero-day-active-attack/167704/ |
| SolarWinds | https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211 |
| ZDNet | https://www.zdnet.com/article/solarwinds-releases-security-advisory-after-microsoft-says-customer-targeted-through-vulnerability |