The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
07/13/2021

SUBJECT:
A Vulnerability in SolarWinds Serv-U Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in SolarWinds Serv-U, which could result in remote code execution. SolarWinds Serv-U is an FTP server software for secure file transfer. Successful exploitation of this vulnerability could allow for remote code execution within the context of a privileged process. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
Microsoft has provided evidence of limited, targeted customer impact, though SolarWinds does not currently have an estimate of how many customer may be directly affected by the vulnerability.

SYSTEMS AFFECTED:

- SolarWinds Serv-U versions prior to Serv-U 15.2.3 HF2

RISK:
Government:

- Large and medium government entities: **High**
- Small government: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in SolarWinds Serv-U, which could result in remote code execution. SolarWinds Serv-U is prone to a remote memory escape vulnerability that could allow a threat actor to run arbitrary code within the context of a privileged process. Depending

on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by SolarWinds to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

SolarWinds:

https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211

BleepingComputer:

https://www.bleepingcomputer.com/news/security/solarwinds-patches-critical-serv-u-vulnerability-exploited-in-the-wild/

ZDNet:

https://www.zdnet.com/article/solarwinds-releases-security-advisory-after-microsoft-says-customer-targeted-through-vulnerability/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35211

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.