Hive Pro

THREAT ADVISORY

Threat Actors are actively exploiting a SolarWinds Zero-Day	TA202125
Threat Level AMBER	**Publish Date –** July 13, 2021

A zero-day vulnerability(CVE-2021-35211) that impacts the Serv-U Managed File Transfer and Serv-U Secure FTP, is been exploited by multiple threat actors. The PoC of this exploited vulnerability was given to SolarWinds by Microsoft. SolarWinds has released a patch for the same.

Vulnerability Details

CVE ID	Affected Versions	Affected CPEs	Vulnerability Name	CWE ID
CVE-2021-35211	Serv-U 15.2.3 HF1 and all prior Serv-U versions	cpe:2.3:a:solarwinds:serv-u_ftp_server:15.2:*:*:*:*:*:*:*, cpe:2.3:a:solarwinds:serv-u_ftp_server:15.1:*:*:*:*:*:*:*	Serv-U Remote Memory Escape Vulnerability	CWE-119

Indicator of Compromise

Type	Value
IP Address	98.176.196.89 68.235.178.32 208.113.35.58

Patch Link

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

References

https://www.rapid7.com/blog/post/2021/07/12/solarwinds-serv-u-ftp-and-managed-file-transfer-cve-2021-35211-what-you-need-to-know/
https://thehackernews.com/2021/07/a-new-critical-solarwinds-zero-day.html