Hive Pro

THREAT ADVISORY

SolarWinds Serv-U vulnerability exploited to deliver Log4j attack

TA2022016

Threat Level RED

Publish Date – Jan 24, 2022

SolarWinds is affected by a vulnerability (CVE-2021-35247) due to improper input validation when processing LDAP queries in the Serv-U web login screen. Serv-U versions up to 15.2.5 are affected by this flaw and were fixed in version 15.3.

A threat actor used this vulnerability to send a manipulated LDAP query with unsanitized data to target Serv-U using the Log4j vulnerability. The attempt failed because Serv-U does not use Log4j code and the authentication target – LDAP (Microsoft Active Directory) – is not vulnerable to Log4j attacks.

HivePro threat researchers advise customers to patch the vulnerability using the link given below.

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-35247	SolarWinds Serv-U Earlier than 15.2.5	cpe:2.3:a:solarwinds:serv-u:*:*:*:*:*:*:*:*	SolarWinds Serv-U web login screen code execution	CWE-20, CWE-90

Patch Link

https://documentation.solarwinds.com/en/success_center/servu/content/servu-iug-upgrade.htm

References

https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35247
https://threatpost.com/microsoft-log4j-attackssolarwinds-serv-u-bug/177824/
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/#CVE-2021-35247