Microsoft: SolarWinds fixes Serv-U bug exploited for Log4j attacks

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** January 19, 2022 05:32 PM **0**

SolarWinds has patched a Serv-U vulnerability discovered by Microsoft that threat actors actively used to propagate Log4j attacks to internal devices on a network.

Microsoft says they discovered the vulnerability during their monitoring of the Log4j attacks.

The bug is an input validation vulnerability discovered by Microsoft security researcher Jonathan Bar Or (https://twitter.com/yo_yo_yo_jbo) that allows an attacker to create a query and send it unsanitized over the network.

"During our sustained monitoring of threats taking advantage of the Log4j 2 vulnerabilities, we observed activity related to attacks being propagated via a previously undisclosed vulnerability in the SolarWinds Serv-U software," Microsoft explains in an update to their Log4J advisory (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).

"We discovered that the vulnerability, now tracked as CVE-2021-35247, is an input validation vulnerability that could allow attackers to build a query given some input and send that query over the network without sanitation."

Yesterday, SolarWinds issued an advisory for CVE-2021-35247 and released Serv-U 15.3 to fix the vulnerability.

"The Serv-U web login screen to LDAP authentication was allowing characters that were not sufficiently sanitized," reads SolarWinds advisory (https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35247).

"SolarWinds has updated the input mechanism to perform additional validation and sanitization."

However, SolarWinds states that no downstream effect has been detected "as the LDAP servers ignored improper characters," contradicting Microsoft's report.

At this point, it is unclear if the threat actors attempted to use the vulnerability but failed or if Log4j attacks were successfully propagated as indicated by Microsoft.

Threat actors have previously abused Serv-U vulnerabilities to perform Conti ransomware attacks (https://www.bleepingcomputer.com/news/security/clop-gang-exploiting-solarwinds-serv-u-flaw-in-ransomware-attacks/) and other undisclosed attacks (https://www.bleepingcomputer.com/news/security/solarwinds-patches-critical-serv-u-vulnerability-exploited-in-the-wild/).

BleepingComputer has reached out to Microsoft and SolarWinds with further questions but has not heard back at this time.

Related Articles:

Microsoft Defender Log4j scanner triggers false positive alerts (https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-log4j-scanner-triggers-false-positive-alerts/)

Microsoft Azure App Service flaw exposed customer source code (https://www.bleepingcomputer.com/news/security/microsoft-azure-app-service-flaw-exposed-customer-source-code/)

Windows Server 2019 OOB update fixes reboots, Hyper-V, ReFS bugs (https://www.bleepingcomputer.com/news/microsoft/windows-server-2019-oob-update-fixes-reboots-hyper-v-refs-bugs/)

Microsoft leak: Third-party widgets coming soon to Windows 11 (https://www.bleepingcomputer.com/news/microsoft/microsoft-leak-third-party-widgets-coming-soon-to-windows-11/)

New Windows KB5009543, KB5009566 updates break L2TP VPN connections (https://www.bleepingcomputer.com/news/microsoft/new-windows-kb5009543-kb5009566-updates-break-l2tp-vpn-connections/)