SLP Vulnerability Allows DoS Attacks With Amplification Factor of 2,200



A high-severity vulnerability in the Service Location Protocol (SLP) can be exploited to launch denial-of-service (DoS) attacks with a high amplification factor, security researchers at Bitsight and Curesec warn.

A legacy internet protocol created in 1997, SLP is used for local network service discovery, without prior configuration, and can be scaled from small to large enterprise networks. The protocol was not intended to be exposed to the public internet.

Tracked as CVE-2023-29552 (CVSS score of 8.6), the newly disclosed vulnerability exists because SLP allows unauthenticated, remote attackers to register arbitrary services.

“This could allow the attacker to use spoofed UDP traffic to

conduct a denial-of-service attack with a significant amplification factor," a NIST advisory explains.

The vulnerability allows for a DoS amplification factor of 2,200, Bitsight says. This is possible because attackers could combine a typical reflective DoS amplification attack with service registration to increase the amount of traffic sent to the victim.

"Assuming a 29-byte request, the amplification factor is roughly between 1.6X and 12X. However, SLP allows an unauthenticated user to register arbitrary new services, meaning an attacker can manipulate both the content and the size of the server reply, resulting in a maximum amplification factor of over 2200X due to the roughly 65,000-byte response given a 29-byte request," Bitsight explains.

To exploit the vulnerability for DoS amplification, an attacker needs to find an SLP server on UDP port 427, register services until SLP denies more entries, send a request to the service by spoofing the victim's IP as the origin, and then repeat the last step while the attack is ongoing.

"Depending on the software and/or system being used, the size of the reply can potentially reach the practical limit of a single UDP packet, which is typically 65,536 bytes," Bitsight notes.

In February 2023, more than 2,000 global companies were using SLP, with over 54,000 SLP instances found to be accessible from the internet. According to Curesec, currently there are roughly 34,000 exploitable systems with SLP.

Bitsight says it has identified vulnerable instances belonging to Fortune 1000 organizations in the finance, insurance, healthcare, hospitality, manufacturing, technology, telecommunications, and transportation sectors.

More than 670 different product types were found vulnerable,

including IBM Integrated Management Module (IMM), HP printers, Konica Minolta printers, Planex routers, VMware ESXi servers, and many others.

On Tuesday, VMware warned that, while currently supported ESXi releases (ESXi 7.x and 8.x) are not impacted by CVE-2023-29552, releases that are no longer supported, such as 6.7 and 6.5, are vulnerable. Customers are advised to upgrade to a supported release as soon as possible.

According to Cloudflare and Netscout, SLP is likely to soon be abused to amplify distributed denial-of-service (DDoS) attacks, unless organizations take the necessary precautions to secure the SLP instances they use.

Disabling SLP on systems running on untrusted networks should prevent exploitation of CVE-2023-29552. Setting firewall rules to filter traffic on UDP and TCP port 427 should also mitigate the risks associated with the flaw.

On Tuesday, the US Cybersecurity and Infrastructure Security Agency (CISA) urged network administrators to review the available information on CVE-2023-29552 and to “consider disabling or restricting network access to SLP servers” to prevent exploitation.

Related: Mitel Devices Abused for DDoS Vector With Record-Breaking Amplification Ratio

Related: DDoS Attacks Abuse Network Middleboxes for Reflection, Amplification

Related: Researchers Show How Censorship Systems Can Be Abused for DDoS Amplification

SLP Vulnerability Allows DoS Attacks With Amplification Factor of 2,200