corero
[THE DDoS PROTECTION SPECIALISTS]

Corero SmartWall® Threat Advisory

Service Location Protocol (SLP) Reflection/Amplification Attack

Advisory ID: 042623-1
Published: 26 April 2023

Summary

The Service Location Protocol (SLP, RFC 2608) allows an unauthenticated, remote attacker 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, discovered in CVE-2023-29552.

Threat Vector

Researchers from Bitsight and Curesec have discovered a way to abuse SLP to conduct high amplification factor DoS attacks using spoofed source addresses.
Reflective DoS amplification attack leveraging CVE-2023-29552:

- Step 1: The attacker finds an SLP server on UDP port 427.
- Step 2: The attacker registers services until SLP denies more entries.
- Step 3: The attacker spoofs a request to that service with the victim's IP as the origin.
- Step 4: The attacker repeats step three as long as the attack is ongoing.

Reference Links:
Abuse of the Service Location Protocol May Lead to DoS Attacks | CISA
New high-severity vulnerability (CVE-2023-29552) discovered in the Service Location Protocol (SLP) | Bitsight

Recommended Action: Non-SecureWatch Customers

1. To Mitigate SLP Reflection Attack

SLP Reflection attacks utilize UDP source port 427. This attack traffic is detected and mitigated by SmartWall's automatic zero-day Smart-Rule protection.

To further improve protection from this vector, Corero recommends the following configuration setting is applied to your CMS Protection policy under the Reflection Smart-Rules:

Rule-cns-002091: Add source port 427

To make this change, please refer to the CMS User Guide for your software version, which can be found in the Downloads section of the Corero Customer Support Portal. If assistance is still required, then please raise a support case.

2. To Prevent Being Abused as a Reflector

For customers with SLP public, Corero also recommends that customer firewalls should be configured to filter traffic destined to UDP port 427. This will prevent external attackers from accessing the SLP service.

SmartWall DDoS protection solutions mitigate a wide range of known and zero-day attacks, all while maintaining the availability of applications and services being protected and without disrupting the

delivery of legitimate traffic. They are designed to handle large DDoS floods, reflective amplified spoof attacks (such as SADP), as well as attacks that are typically too low, or short, to be mitigated manually, or by traditional out-of-band solutions.

Please contact Corero Support if you have any questions

Recommended Action: SecureWatch Managed Customers

The SecureWatch team is proactively verifying and optimizing protection for SecureWatch Managed systems, so no customer action is required.