Radware Cybersecurity Advisory

SLP DDoS Reflection and Amplification CVE-2023-29552

May 2, 2023

Researchers discovered a new vulnerability in the Service Location Protocol (SLP) that allows malicious actors to leverage systems exposed on the internet in reflection and amplification denial-of-service attacks against arbitrary targets. Network behavioral algorithms can detect SLP floods, and protections can filter malicious packets without affecting legitimate traffic. However, given the massive potential for amplification—up to 2,200x—the most important issue organizations will face are vast volumes of traffic that can saturate their internet links. Cloud DDoS mitigation will, for most businesses, be required to adequately protect against SLP amplification attacks.

Background

While collecting evidence in a recent VMware ESXi attack by a random ransomware group, researchers from **Curesec**, in collaboration with **Bitsight**, discovered a DDoS amplification vulnerability in the SLP. This protocol, defined in RFC 2608 and RFC 3224, allows computers and other devices to find services in a local area network. The vulnerability is tracked as **CVE-2023-29552** and was **disclosed** in coordination with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

SLP was designed by Sun Microsystems in 1997 and has since been superseded by more modern alternatives like UPnP, mDNS/Zeroconf and WS-Discovery. While the alternatives are more recent, they also are known to be prone to abuse in DDoS amplification attacks. The UPnP SSDP protocol provides up to 30x amplification, mDNS up to 5x, and WS-Discovery up to 500x.

According to the researchers, SLP can reach amplification factors up to 2200x, putting it in the range of **Memcached** DDoS amplification attack vectors. Like Memcached, SLP was never intended to be exposed on the public internet. It was only meant for use in local area networks.

The attack

To leverage SLP in reflection attacks, an attacker only needs to send crafted UDP packets, source-spoofed with the victim's IP address, to a server listening on UDP port 427. To leverage amplification, the attackers need to go through a one-time setup phase to fill the server's response buffer by registering services until the SLP server denies more entries. The attacker can manipulate both the content and size of the server's reply messages by registering arbitrary new services. During the setup phase of the attack, the interaction between the attacker and the server would look like a service registration loop until the server buffer is full, followed by arbitrary spoofed requests. Depending on the software and/or system being used, the reply's size can reach the practical limit of a single UDP packet, which is 65,536 bytes, and will result in fragmented UDP traffic when transmitted over the internet.

Risk

In February, the researchers identified over 54,000 SLP instances that attackers could leverage to launch denial-of-service attacks. The vulnerable endpoints include VMware ESXi hypervisors, Konica Minolta printers, Planex routers, IBM Integrated Management Modules (IMM), SMC IPMI, and others. Most SLP-enabled endpoints are server-class computers running older, unpatched versions of the VMWare ESXi bare-metal hypervisor.

Collateral Impact

SLP reflection and amplification attacks can significantly impact organizations that expose SLP-enabled systems online. The impact can include partial or complete interruption of applications and services running on VMWare or cause service interruptions in printer or routing devices.

Mitigation

The resulting amplification attack traffic will resemble most reflection and amplification floods. The packet flood will consist of packets with consistent source ports and specific source IP addresses—from the abused server and service—combined with random destination ports. The destination IP can also be randomized within the range of the targeted subnet if the attacker leverages a carpet-bombing technique.

Network behavioral detection algorithms can detect and filter malicious packets. However, given the massive potential for amplification (2,200x), the most important issue organizations will face are huge volumes of traffic that can saturate internet links. Consequently, diversion to a cloud DDoS mitigation service will, in most cases, be required to adequately protect against SLP amplification attacks.

VMWare **provided** patched software versions for organizations that run SLP-enabled systems that prevent SLP-enabled ESXi servers from being abused through CVE-2023-29552. VMWare customers should contact their vendor for remediation instructions. Operators of other SLP-enabled systems such as print servers should contact relevant vendors for remediation instructions.

Reasons for concern

The newly discovered SLP vulnerability provides one more reflection and amplification attack vector in the toolset of malicious actors. SLP adds to a long list of known DDoS amplification attack vectors such as DNS, NTP, SSDP, WSD, CLDAP and many others. Network behavioral detection algorithms are able to detect and filter malicious amplification traffic. However, given the risk of up to 2,200x amplification, organizations should be concerned about high-volume traffic that can saturate internet links. Consequently, diversion to a cloud DDoS mitigation service will, in most cases, be required to adequately protect against SLP amplification attacks.

Radware Cybersecurity Advisory

SLP DDoS Reflection and Amplification CVE-2023-29552

May 2, 2023

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection - Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation - Promptly protect against unknown threats and zero-day attacks

A Cyber-Security Emergency Response Plan - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options - on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.