Service Location Protocol (SLP) Denial-of-Service Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-29552
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-25 16:15:00 UTC
Updated	2023-05-04 19:07:00 UTC
Description	The Service Location Protocol (SLP, RFC 2608) allows an unauthenticated, remote attacker to register arbitrary services. T

Risk And Classification

EPSS: 0.929620000 probability, percentile 0.997790000 (date 2026-04-21)

CISA KEV: Listed on 2023-11-08; due 2023-11-29; ransomware use Unknown

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	IETF
Product	Service Location Protocol (SLP)
Name	Service Location Protocol (SLP) Denial-of-Service Vulnerability
Required Action	Apply mitigations per vendor instructions or disable SLP service or port 427/UDP on all systems running on untrusted networks, including those directly connected to the Internet.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on the patching status. For more information please see https://www.bitsight.com/blog/new-high-severity-vulnerability-cve-2023-29552-discovered-service-location-protocol-slp and https://www.cisa.gov/news-events/alerts/2023/04/25/abuse-service-location-protocol-may-lead-dos-attacks.; https://nvd.nist.gov/vuln/detail/CVE-2023-29552

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Smi-s Provider	-	All	All	All
Application	Service Location Protocol Project	Service Location Protocol	-	All	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All

Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	15	All	All	All
Operating System	Suse	Linux Enterprise Server	15	All	All	All
Application	Suse	Manager Server	-	All	All	All
Operating System	Vmware	Esxi	All	All	All	All

References

Reference
CVE-2023-29552 Service Location Protocol Vulnerability in NetApp Products | NetApp Product Security
CVE-2023-29552 Service Location Protocol-Denial of Service Amplification Attack - Cureblog
Security Vulnerability: New SLP based traffic amplification attack (CVE-2023-29552) | Support | SUSE
New high-severity vulnerability (CVE-2023-29552) discovered in the Service Location Protocol (SLP) | Bitsight
VMware Response to CVE-2023-29552 - reflective Denial-of-Service (DoS) amplification vulnerability in SLP - VMware Security Blog - VMwar
Abuse of the Service Location Protocol May Lead to DoS Attacks | CISA
GitHub - curesec/slpload: service location protocol amplified denial of service attack verification tool
RFC 2608 - Service Location Protocol, Version 2
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

216311 VMware ESXi 6.5 Reflective Denial of Service (DoS) Amplification Vulnerability in SLP

216312 VMware ESXi 6.7 Reflective Denial of Service (DoS) Amplification Vulnerability in SLP