Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Outdated Internet Protocol Vulnerable to Massive DoS

Date of Publication	Last updated date	Admiralty Code	TA Number
May 2, 2023	November 10, 2023	A1	TA2023206

Summary

First Seen: April 25, 2023
Affected Product: IETF Service Location Protocol
Top 10 Vulnerable Countries: United States, France, United Kingdom, Italy, Japan, Brazil, Germany, Netherlands, Canada, Spain
Vulnerable Industries: Legal, Credit Union, Engineering, Retail, Consumer Goods, Healthcare / Wellness, Food Production, Manufacturing, Tourism/Hospitality, Insurance, Real Estate, Nonprofit/ NGO, Energy/Resources, Media/Entertainment, Transportation, Finance, Business Services, Utilities, Government/Politics, Telecommunications, Education, Technology
Impact: Denial of Service Attack could cause a loss of up to $120,000

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-29552	Service Location Protocol (SLP) Denial-of-Service Vulnerability	IETF Service Location Protocol (SLP)	✗	✓	✗

Vulnerability Details

#1 In April 2023, a serious vulnerability (known as CVE-2023-29552) was discovered in the Service Location Protocol (SLP), which is an outdated Internet protocol. SLP is a protocol enabling local area network systems to discover and communicate with each other. If attackers exploit this vulnerability, they can use vulnerable instances to launch very large Denial-of-Service (DoS) amplification attacks that can amplify the attack factor up to 2200 times. This could potentially be one of the largest amplification attacks ever reported. The vulnerability is actively exploited.

#2 Over 2,000 global organizations and more than 54,000 SLP instances, including various devices such as VMware ESXi Hypervisor, Konica Minolta printers, Planex Routers, IBM Integrated Management Module (IMM), and SMC IPMI, were identified as potentially vulnerable to these attacks. Although SLP was not intended to be publicly available on the internet, it has been found in a variety of instances connected to the internet.

#3 VMware has issued several advisories warning users about vulnerabilities affecting SLP in their ESXi products and has disabled SLP by default in ESXi software releases since 2021. In recent months, ransomware groups have taken advantage of a flaw in SLP implementations in campaigns targeting vulnerable organizations. These DoS attacks have resulted in significant financial, reputational, and operational damage. Small to medium-sized businesses (SMBs) typically spend an average of $120,000 due to a DoS attack, while larger organizations may face greater financial losses due to higher disruption costs. Even large multinational corporations are not immune to these attacks - Amazon Web Services (AWS), GitHub, and even nation-states have been victims of DoS attacks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-29552	Service Location Protocol version: 2.0.0	cpe:2.3:a:service_location_protocol:service_location_protocol:*:*:*:*:*:*:*:*	CWE-345

Recommendations

Disable SLP on all systems running on untrusted networks: Organizations should assess whether SLP is necessary for their network requirements. If SLP is not essential, then it should be disabled on all systems running on untrusted networks, especially those connected directly to the Internet. This step will prevent attackers from exploiting the vulnerability and launching DoS amplification attacks.

Configure firewalls to filter traffic on UDP and TCP port 427: If disabling SLP is not possible, then organizations should configure firewalls to filter traffic on UDP and TCP port 427. This step will restrict external access to the SLP service and reduce the attack surface. Additionally, organizations should review their firewall rules regularly to ensure that they are up-to-date and effective in mitigating SLP-related attacks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0040** Impact	**TA0042** Resource Development	**T1498** Network Denial of Service
T1498.002 Reflection Amplification	**T1588.006** Vulnerabilities	**T1588.005** Exploits	**T1588** Obtain Capabilities
T1190 Exploit Public-Facing Application			

References

https://www.bitsight.com/blog/new-high-severity-vulnerability-cve-2023-29552-discovered-service-location-protocol-slp

https://www.cisa.gov/news-events/alerts/2023/04/25/abuse-service-location-protocol-may-lead-dos-attacks

https://blogs.vmware.com/security/2023/04/vmware-response-to-cve-2023-29552-reflective-denial-of-service-dos-amplification-vulnerability-in-slp.html

https://www.rfc-editor.org/rfc/rfc2165.html

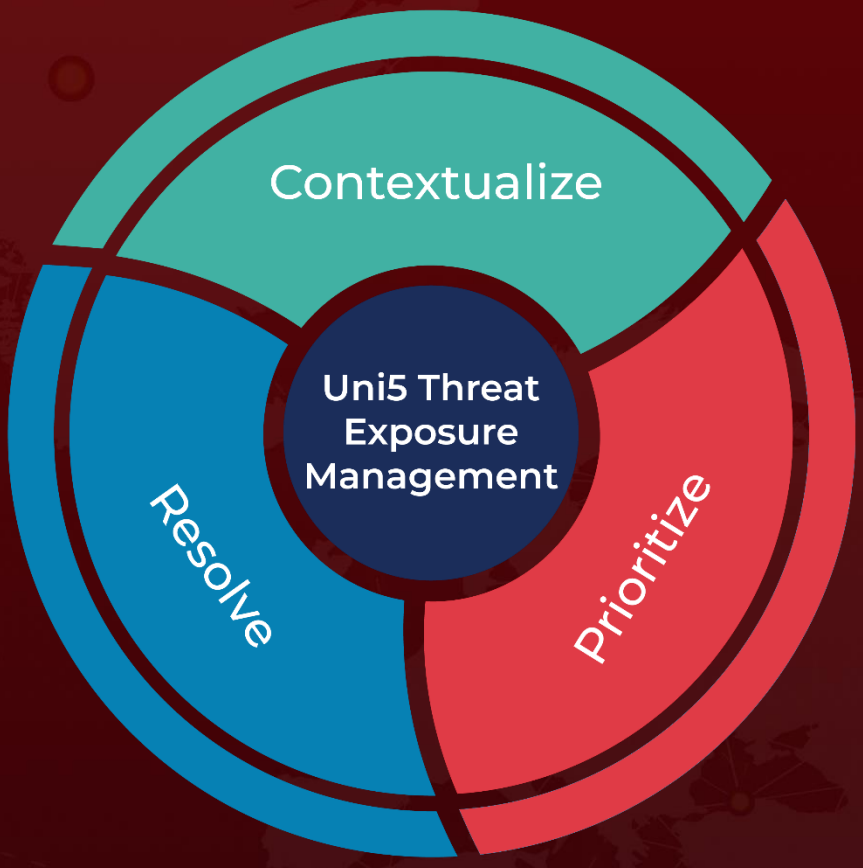
https://www.suse.com/support/kb/doc/?id=000021051

https://www.cisa.gov/news-events/alerts/2023/11/08/cisa-adds-one-known-exploited-vulnerability-catalog

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 2, 2023 • 4:15 AM

More at www.hivepro.com