Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-61932: Critical Lanscope Endpoint Manager Flaw Actively Exploited

Date of Publication	Admiralty Code	TA Number
October 24, 2025	A1	TA2025326

Summary

First Seen: April 2025
Affected Product: Motex LANSCOPE Endpoint Manager
Impact: CVE-2025-61932 is a critical remote code execution vulnerability in Motex's Lanscope Endpoint Manager (on-premises), affecting the Client (MR) and Detection Agent (DA) components. It allows a remote attacker to execute arbitrary code on vulnerable endpoints by sending specially crafted packets, with real-world exploitation observed since April 2025. Versions up to 9.4.7.1 are affected, while patched releases are available, and the management server itself is not impacted. Organizations should urgently apply updates, limit network exposure, and monitor endpoints to prevent compromise.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-61932	Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability	Motex LANSCOPE Endpoint Manager	✓	✓	✓

Vulnerability Details

#1

CVE-2025-61932 is a critical remote code execution (RCE) vulnerability affecting the on-premises version of LANSCOPE Endpoint Manager, specifically its Client program (MR) and Detection Agent (DA) components. The flaw arises from improper verification of the origin of incoming communication requests, allowing a remote attacker to send specially crafted packets, typically via TCP port 443, and execute arbitrary code on vulnerable endpoints.

#2 The vulnerability affects versions up to 9.4.7.1 (and earlier) of the on-premises product. The cloud version is not affected, and the management server component does not require upgrading; only the client and agent modules need patching. Lanscope Endpoint Manager is widely used in Japan and across parts of Asia for enterprise endpoint management, which amplifies the potential impact of exploitation in production environments.

#3 Successful exploitation could lead to full compromise of the endpoint device, enabling an attacker to execute arbitrary code and persist within networks. Given that the flaw can be triggered remotely without authentication or user interaction, it represents a significant threat to enterprise environments.

#4 Active exploitation of CVE-2025-61932 has been observed since April 2025, with attackers using malicious packets to drop backdoors on vulnerable systems, enabling persistent remote control. Organizations using the affected Lanscope components should immediately apply the available patches, restrict client endpoints' exposure to untrusted networks, and monitor inbound traffic and unusual executable activity.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-61932	LANSCOPE Endpoint Manager On-Premise Version 9.4.7.1 and earlier Client Program (MR) Detection Agent (DA)	cpe:2.3:a:motex:lanscope_endpoint_manager:*:*:*:*:*:on-premise:*:*:*	CWE-940

Recommendations

Apply Patches Immediately: Organizations should promptly upgrade the Lanscope Endpoint Manager Client (MR) and Detection Agent (DA) components to the latest patched versions (9.3.2.7–9.4.7.3 or newer) as released by Motex. These updates contain essential fixes that eliminate the code execution flaw exploited in active attacks.

Restrict Network Exposure: Until patching is complete, reduce risk by restricting inbound network access to affected clients and agents. Block or monitor any unexpected traffic, especially to ports such as TCP 443, and ensure only trusted hosts/networks can reach those endpoints.

Monitor Network Traffic: Actively monitor inbound and outbound traffic for unusual activity on TCP port 443, as observed in recent exploitation attempts. Deploy intrusion detection or prevention systems (IDS/IPS) to flag anomalous packets associated with Lanscope clients. Review logs for unexplained connections or recurring traffic patterns that could indicate command-and-control or backdoor behavior.

Review Endpoint Security: Perform comprehensive endpoint scans using trusted EDR or antivirus tools to detect any unauthorized changes, scripts, or executables. Pay special attention to systems running vulnerable client or agent versions that have been connected to external networks. Isolate and investigate any endpoints showing signs of compromise to prevent lateral movement within your environment.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control	TA0042 Resource Development
TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration	TA0004 Privilege Escalation
T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1071.001 Web Protocols	T1071 Application Layer Protocol

T1588.006 Vulnerabilities	T1588.005 Exploits	T1588 Obtain Capabilities	T1068 Exploitation for Privilege Escalation
T1059 Command and Scripting Interpreter	T1210 Exploitation of Remote Services		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	38[.]54[.]56[.]10, 38[.]60[.]212[.]85, 108[.]61[.]161[.]118, 38[.]54[.]56[.]57, 38[.]54[.]88[.]172

Patch Details

The patched versions for CVE-2025-61932 are, 9.3.2.7, 9.3.3.9, 9.4.0.5, 9.4.1.5, 9.4.2.6, 9.4.3.8, 9.4.4.6, 9.4.5.4, 9.4.6.3, and 9.4.7.3. Only the Client (MR) and Detection Agent (DA) require updating.

Link:
https://www.motex.co.jp/news/notice/2025/release251020/

References

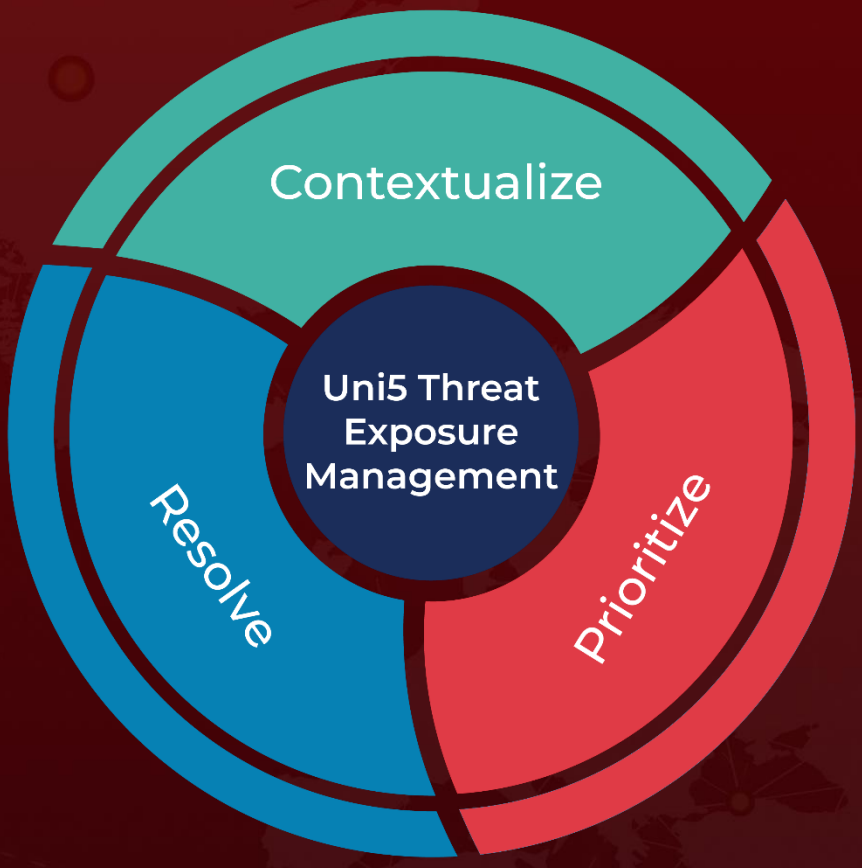
https://www.jpcert.or.jp/newsflash/2025102001.html

https://jvn.jp/jp/JVN86318557/

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

October 24, 2025 . 11:30 AM

More at www.hivepro.com