Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Espionage Ops Exploit Output Messenger Vulnerability

Date of Publication	Admiralty Code	TA Number
May 14, 2025	A1	TA2025147

Summary

First Seen: April 2024
Affected Product: Output Messenger
Threat Actor: Marbled Dust (alias Silicon, Cosmic Wolf, Sea Turtle, Teal Kurma, UNC1326)
Impact: The Türkiye-affiliated espionage group Marbled Dust (Sea Turtle) has been exploiting a zero-day vulnerability, CVE-2025-27920, in Output Messenger to infiltrate systems linked to the Kurdish military in Iraq. Leveraging the directory traversal flaw, the group deployed malicious payloads and a custom GoLang backdoor, gaining covert access to sensitive communications and credentials.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-27920	Output Messenger Directory Traversal Vulnerability	Output Messenger	✓	✗	✓

Vulnerability Details

#1 Since April 2024, a Türkiye-affiliated cyberespionage group known as Marbled Dust, also referred to as Sea Turtle, has been actively exploiting a zero-day vulnerability, tracked as CVE-2025-27920, in Output Messenger a cross-platform messaging application. The group targeted users affiliated with the Kurdish military in Iraq, consistent with its previously observed objectives.

#2 Marbled Dust began by conducting reconnaissance to identify Output Messenger users, selecting victims based on this intelligence. The exploited vulnerability, a directory traversal flaw in the Output Messenger Server Manager application, allows authenticated users to upload malicious files to the server's startup directory. The group leveraged this to deploy a malicious script, OMServerService.vbs, ensuring persistent access.

#3 Output Messenger's server configuration enables administrators to activate an output drive feature, permitting file uploads and downloads. Uploaded files are typically stored in a temporary directory, but the flaw allows authenticated users to manipulate the "name" parameter in upload requests to perform directory traversal and place files outside the intended path.

#4 Upon compromising a server, Marbled Dust exploited Output Messenger's client-server architecture, where clients authenticate, exchange messages, and share files via a central server, to intercept communications, exfiltrate sensitive data, and impersonate legitimate users. This activity resulted in operational security risks, internal system exposure, and credential compromise.

#5 Initial access was likely obtained via DNS hijacking and typo-squatted domains, longstanding tactics in Marbled Dust's arsenal for credential harvesting and reuse. Following server compromise, the group deployed a custom GoLang-based backdoor masquerading as a legitimate file.

#6 GoLang's cross-platform compatibility made it an effective tool for persistent access. The backdoor connected to a hardcoded, attacker-controlled command-and-control server, enabling data exfiltration and the delivery of follow-on payloads, ensuring continued covert access to compromised environments.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-27920	Output Messenger before 2.0.63	cpe:2.3:a:output_messenger:output_messenger:-:*:*:*:*:*:*:*	CWE-22

Recommendations

Immediate Upgrade to Fixed Version: All Output Messenger users should urgently upgrade to version V2.0.63 or later, where CVE-2025-27920 has been resolved. Delaying this update leaves systems vulnerable to active exploitation.

Audit Server Configurations: Review Output Messenger Server Manager settings, particularly those related to file upload and output drive permissions. Disable unnecessary features or restrict access to trusted users only.

Harden File Upload Handling: Implement strict validation and sanitization of file uploads. Restrict upload directories and monitor for suspicious file paths or unauthorized changes within the server's startup directory.

Network Segmentation and Traffic Monitoring: Segregate critical messaging infrastructure from other sensitive systems. Deploy intrusion detection systems (IDS) and monitor for unusual outbound connections or traffic to known malicious domains.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration
TA0042 Resource Development	T1078 Valid Accounts	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1037 Boot or Logon Initialization Scripts	T1036 Masquerading	T1212 Exploitation for Credential Access
T1046 Network Service Discovery	T1071.004 DNS	T1041 Exfiltration Over C2 Channel	T1082 System Information Discovery
T1027 Obfuscated Files or Information	T1587.004 Exploits	T1574 Hijack Execution Flow	T1587 Develop Capabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	OMServerService.vbs, OMServerService.exe, OM.vbs
Domain	hxxps[:]//api[.]wordinfos[.]com

Patch Details

All Output Messenger administrators are strongly advised to immediately upgrade to V2.0.63 to prevent active exploitation of this vulnerability. Systems running older versions remain at risk of compromise.

Link:
https://www.outputmessenger.com/cve-2025-27920/

References

https://www.microsoft.com/en-us/security/blog/2025/05/12/marbled-dust-leverages-zero-day-in-output-messenger-for-regional-espionage/

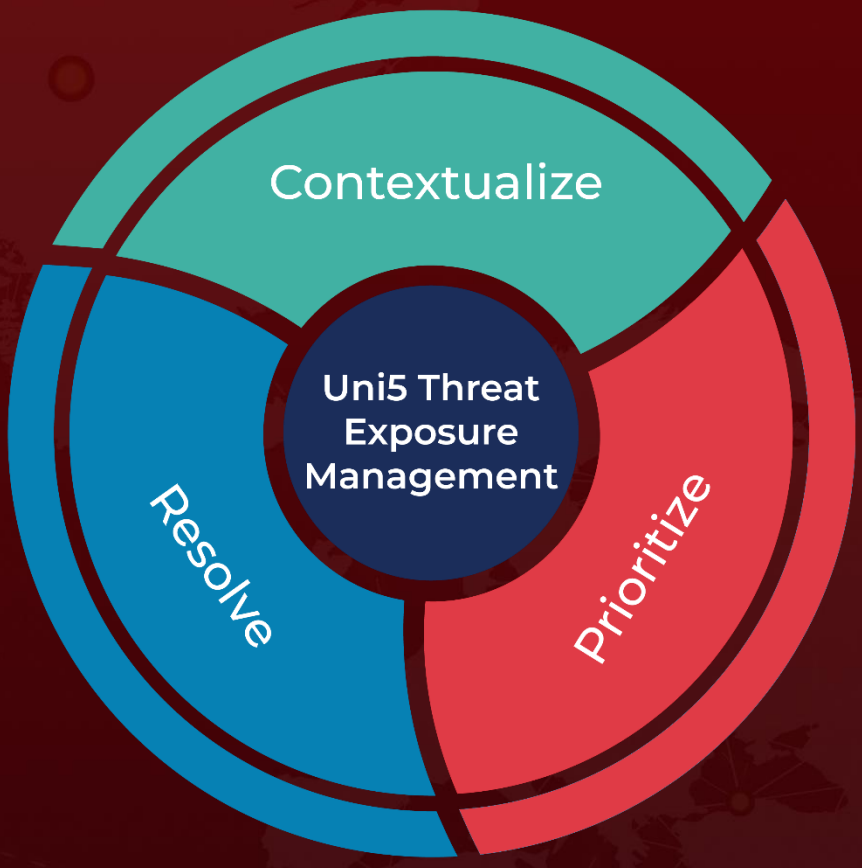
https://www.outputmessenger.com/release-notes/windows/

https://hivepro.com/threat-advisory/unveiling-the-sea-turtle-cyber-espionage-campaign/

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 14, 2025 • 4:00 AM

More at www.hivepro.com