Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Fake LDAPNightmare Exploit on GitHub Spreads Infostealer Malware

Date of Publication	Admiralty Code	TA Number
January 13, 2025	A1	TA2025010

Summary

First Seen: January 1, 2025
Affected Product: Microsoft Windows
Impact: Cybercriminals are spreading infostealer malware disguised as a PoC exploit for the CVE-2024-49113 (aka LDAPNightmare) vulnerability via fake GitHub repositories. The malicious file, "poc.exe," deploys scripts that collect sensitive system data and exfiltrate it to a remote FTP server. This tactic targets security researchers by exploiting trusted platforms like GitHub. Users should verify sources, review code, and use security tools to avoid these kind of threats.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-49113	LDAPNightmare (Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability)	Microsoft Windows	✗	✗	✓
CVE-2024-49112	LDAPBleed (Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability)	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

A malicious campaign has emerged in which cybercriminals distribute information-stealing malware disguised as a proof-of-concept (PoC) exploit for the LDAPNightmare vulnerability (CVE-2024-49113). The attackers created deceptive GitHub repositories that appear to offer legitimate PoC exploits. However, instead of actual exploit code, these repositories contain a UPX-packed executable named "poc.exe." This file, when executed, runs a malicious PowerShell script that establishes persistence on the victim's system by creating a scheduled task that repeatedly executes an encoded script.

#2

This script downloads additional malware payloads hosted on Pastebin. Once executed, the malware collects sensitive system information, including system details, running processes, directory contents, network configurations, and installed software updates. The harvested data is compressed into a ZIP file and exfiltrated to a remote FTP server using hardcoded credentials. This stealthy data theft enables attackers to collect extensive information from infected systems, potentially facilitating further cyberattacks or breaches.

#3

Additionally, similar to the CVE-2024-49113 vulnerability, CVE-2024-49112 also affects Windows Lightweight Directory Access Protocol (LDAP). With proof-of-concept (PoC) exploits already available, these vulnerabilities pose a significant risk of future exploitation. To mitigate this risk, it is strongly recommended to apply patches for both CVE-2024-49112 and CVE-2024-49113, addressed in the December 2024 Patch Tuesday updates, to prevent potential exploitation and strengthen system security.

#4

The use of GitHub as a distribution platform for this malware highlights a growing trend where attackers exploit trusted platforms to spread malicious software. By disguising malware as security tools or PoC exploits, cybercriminals target cybersecurity researchers and IT professionals who are more likely to download and run these files. This tactic significantly increases the risk of successful infections and data exfiltration while undermining trust in open-source communities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-49113	Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-125
CVE-2024-49112	Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-190

Recommendations

Verify the Source of Downloads: Always download proof-of-concept (PoC) exploits or security tools from trusted and reputable sources. Check if the repository belongs to well-known cybersecurity researchers or verified organizations. Avoid downloading files from unknown or suspicious accounts.

Review and Analyze Code Before Execution: Carefully examine the code for signs of obfuscation, suspicious scripts, or unexpected binaries. Look out for encoded PowerShell commands, packed executables (e.g., UPX-packed files), or automated tasks that could indicate malicious behavior.

Use Security Tools to Scan Files: Before executing any downloaded file, scan it with updated antivirus or endpoint protection tools. Additionally, upload the file to online malware scanning services like VirusTotal to detect hidden threats.

Isolate Testing Environments: Run unverified PoC exploits in isolated, controlled environments such as virtual machines (VMs) or sandboxed systems. This prevents malware from affecting critical systems if the file turns out to be malicious.

Monitor Network Activity for Anomalies: Use network monitoring tools to detect unusual outbound connections, especially to unknown FTP servers or suspicious domains. Immediate investigation of unexpected network activity can prevent data exfiltration.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0042 Resource Development	TA0002 Execution	TA0007 Discovery
TA0003 Persistence	TA0010 Exfiltration	TA0005 Defense Evasion	TA0004 Privilege Escalation
TA0001 Initial Access	T1588.006 Vulnerabilities	T1588 Obtain Capabilities	T1588.005 Exploits
T1059.001 PowerShell	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1036 Masquerading
T1048 Exfiltration Over Alternative Protocol	T1082 System Information Discovery	T1543 Create or Modify System Process	T1059 Command and Scripting Interpreter

T1048 Exfiltration Over Alternative Protocol	T1082 System Information Discovery	T1543 Create or Modify System Process	T1203 Exploitation for Client Execution
T1566 Phishing	T1204 User Execution	T1203 Exploitation for Client Execution	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	Ef4ba8eef919251f7502c7e66926bb3a5422065b, d4a35487b95cc2b44395047717358bb2863a5311
URLs	ftp[:]//ftp[.]drivehq[.]com/wwwhome/, ftp[:]//ftpupload[.]net/htdocs, hxxps[:]//pastebin[.]com/raw/9TxS7Ldc

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49113

References

https://www.trendmicro.com/en_us/research/25/a/information-stealer-masquerades-as-ldapnightmare-poc-exploit.html

https://www.catonetworks.com/blog/cato-ctrl-threat-brief-cve-2024-49112-and-cve-2024-49113-ldap-vulnerabilities/

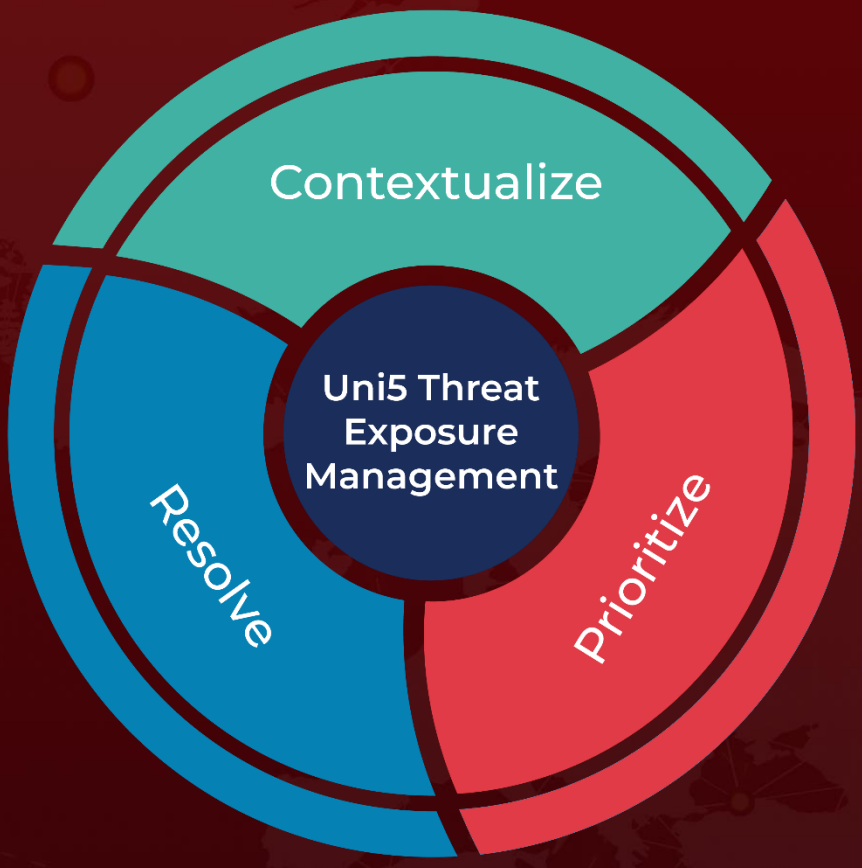
https://github.com/SafeBreach-Labs/CVE-2024-49113

https://github.com/tnkr/poc_monitor

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

January 13, 2025 • 6:30 AM

More at www.hivepro.com