

**HiveForce Labs**

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Cleo Zero-Day File Transfer Vulnerabilities Exploited in the Wild**

**Date of Publication**

December 11, 2024

**Last Update Date**

December 16, 2024

**Admiralty Code**

A1

**TA Number**

TA2024459

# Summary

**First Seen:** October 2024





**Targeted Industries:** Consumer products, Food, Trucking, and Shipping

**Malware:** CIOp

**Affected Products:** Cleo Harmony, Cleo VLTrader, Cleo LexiCom

**Impact:** Critical zero-day vulnerabilities, CVE-2024-50623 and CVE-2024-55956, have been identified in Cleo's file transfer products: Harmony, VLTrader, and LexiCom. These flaws are currently being actively exploited by threat actors, enabling unrestricted file uploads and downloads, which can be leveraged to achieve remote code execution (RCE). The vulnerabilities pose a significant risk to organizations relying on these tools for secure file transfers. The CIOp ransomware gang is found exploiting these flaws in the wild.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-50623	Cleo Multiple Products Unrestricted File Upload Vulnerability	Cleo Harmony, Cleo VLTrader, Cleo LexiCom			
CVE-2024-55956	Cleo Multiple Products Remote Code Execution Vulnerability	Cleo Harmony, Cleo VLTrader, Cleo LexiCom			

# Vulnerability Details

## #1

A critical zero-day vulnerability, CVE-2024-50623, has been identified in Cleo's widely used file transfer solutions, including Harmony, VLTrader, and LexiCom. This flaw, an unrestricted file upload and download vulnerability, could enable remote code execution. Threat actors are actively exploiting this weakness in the wild.

## #2

Cleo's software is typically installed in the root of the file system, with subdirectories like logs, host, and autorun. The attack chain begins with the introduction of a malicious file, autorun\healthchecktemplate.txt, which the software automatically reads, interprets, and executes. This entry point is used to drop additional files, including a crafted .ZIP archive containing a mail.xml file, which leverages the software's legitimate "Import" functionality to execute arbitrary code.

## #3

In one instance of exploitation, attackers used a main.xml file to invoke PowerShell commands, establishing a foothold in the system. Post-execution, the attackers deleted artifacts such as healthchecktemplate.txt and malicious JAR files to maintain stealth. Over 10 compromised Cleo servers have been identified across sectors including consumer products, food, trucking, and shipping, with evidence of exploitation dating back to early December.

## #4

CVE-2024-55956, the other flaw in Cleo's Autorun directory, has further heightened security concerns. This flaw enables attackers to execute arbitrary bash or PowerShell commands, granting them the ability to achieve RCE. Following successful exploitation, attackers have been observed deploying modular Java-based backdoors to establish persistent access, exfiltrate sensitive data, and facilitate lateral movement within compromised networks. Notably, the ClOp ransomware gang has been identified as a key actor exploiting the flaws, leveraging it to expand their reach and inflict significant damage on targeted systems.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-50623	Cleo Harmony (versions upto 5.8.0.21) Cleo VLTrader (versions upto 5.8.0.21) Cleo LexiCom (versions upto 5.8.0.21)	cpe:2.3:a:cleo:vltrader:*:*:*:* :*:*:* cpe:2.3:a:cleo:lexicom:*:*:*:* :*:*:* cpe:2.3:a:cleo:harmony:*:*:* :*:*:*:*	CWE-434
CVE-2024-55956	Cleo Harmony (prior to version 5.8.0.24) Cleo VLTrader (prior to version 5.8.0.24) Cleo LexiCom (prior to version 5.8.0.24)	cpe:2.3:a:cleo:vltrader:*:*:*:* :*:*:* cpe:2.3:a:cleo:lexicom:*:*:*:* :*:*:* cpe:2.3:a:cleo:harmony:*:*:* :*:*:*:*	-

# Recommendations



**Apply Updated Patches Immediately:** Update your Cleo instances to the latest version to address the vulnerabilities.



**Disable Autorun Feature:** It is strongly advised to disable the autorun feature in Cleo's Harmony, VLTrader, and LexiCom software. Disabling autorun prevents the automatic execution of malicious scripts or commands introduced through unauthorized file writes.



**Limit Network Access:** Limit public exposure of Cleo software by placing instances behind firewalls or restricting access to trusted IP ranges.



**Implement Network Monitoring:** Use network monitoring tools to identify and respond to suspicious activities, particularly from administrative accounts. Detecting unauthorized access early can prevent further exploitation.



**Enable File and Process Monitoring:** Use endpoint detection tools to monitor for suspicious file activity, especially related to the autorun directory and PowerShell commands.

## Potential MITRE ATT&CK TTPs

<b>TA0042</b> Resource Development	<b>TA0001</b> Initial Access	<b>TA0002</b> Execution	<b>TA0003</b> Persistence
<b>TA0005</b> Defense Evasion	<b>TA0007</b> Discovery	<b>TA0008</b> Lateral Movement	<b>TA0011</b> Command and Control
<b>T1588</b> Obtain Capabilities	<b>T1588.006</b> Vulnerabilities	<b>T1190</b> Exploit Public-Facing Application	<b>T1566</b> Phishing
<b>T1059</b> Command and Scripting Interpreter	<b>T1059.001</b> PowerShell	<b>T1070</b> Indicator Removal	<b>T1105</b> Ingress Tool Transfer
<b>T1082</b> System Information Discovery	<b>T1133</b> External Remote Services	<b>T1033</b> System Owner/User Discovery	<b>T1482</b> Domain Trust Discovery
<b>T1069</b> Permission Groups Discovery	<b>T1550</b> Use Alternate Authentication Material	<b>T1550.002</b> Pass the Hash	

# ✂ Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	176[.]123[.]5[.]126, 5[.]149[.]249[.]226, 185[.]181[.]230[.]103, 209[.]127[.]12[.]38, 181[.]214[.]147[.]164, 192[.]119[.]99[.]42, 89[.]248[.]172[.]139, 176[.]123[.]10[.]115, 185[.]162[.]128[.]133, 185[.]163[.]204[.]137, 45[.]182[.]189[.]102
Files	60282967-dc91-40ef-a34c-38e992509c2c[.]xml, healthchecktemplate[.]txt, healthcheck[.]txt

## ✂ Patch Details

Cleo has addressed the flaws in the latest version, update your instances to the Version 5.8.0.24.

Link: <https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956>

<https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623>

## ✂ References

<https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild>

<https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623>

<https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956>

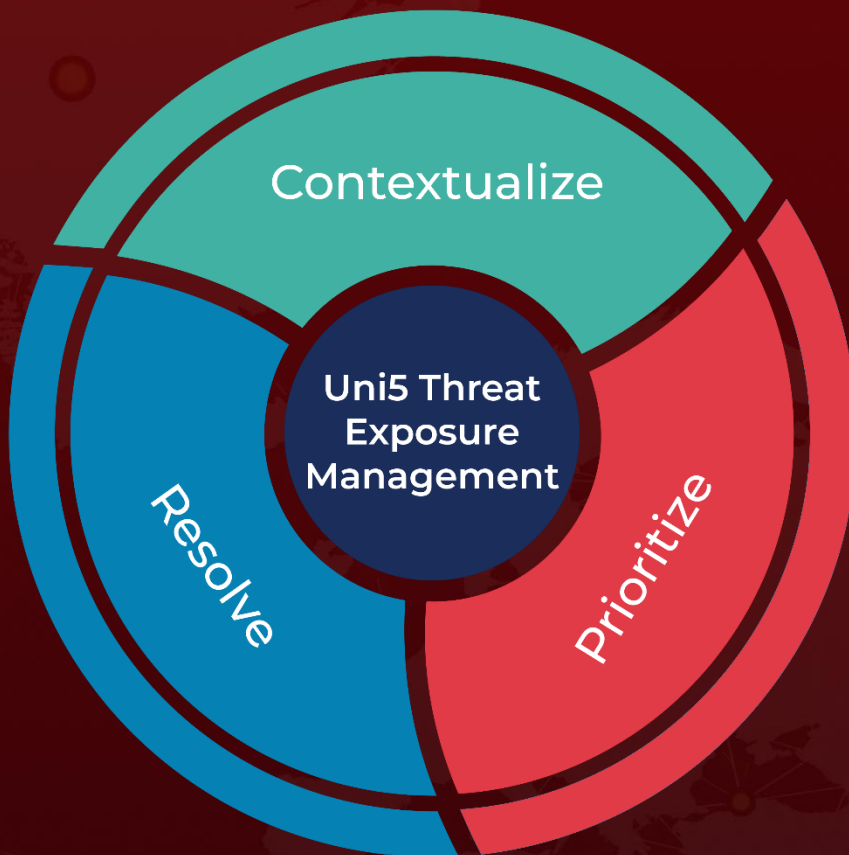
<https://socradar.io/cleo-file-transfer-vulnerabilities-cl0ps-attack-vector/>



# 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

**December 11, 2024 • 6:40 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)