CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
19 December 2024

Cleo's Harmony, VLTrader, and Lexicom Multiple Zero-Day Vulnerabilities

Cleo | Ransomware | RCE | PowerShell

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two critical vulnerabilities known as CVE-2024-5062 (CVSS 9.8)[1] and CVE-2024-5596 (CVSS 9.8).[2] These vulnerabilities affect Cleo's Harmony, VLTrader, and Lexicon file transfer software. Multiple sources have confirmed both CVEs are being actively exploited in ransomware attacks, to possibly include Cl0p Ransomware Group.[3,4,5,6] Affected versions include:

- 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)[7]

CVE-2024050623 is an unrestricted file upload and download vulnerability that can lead to remote code execution with elevated privileges.[8] CVE-2024-5596 is an unrestricted file upload vulnerability that could allow an unauthenticated user to import and execute arbitrary bash or PowerShell commands on the host system by leveraging the default settings of the Autorun directory. [9]

Cleo first published a security update back in October 2024 that addressed CVE-2024-50623 for versions prior to 5.8.0.21.[10] However, Huntress security researchers were able to recreate the proof of concept and found the patch to be ineffective.[11] Since then, a new CVE identifier, CVE-2024-5596, has been assigned to the additional discovered vulnerability and Cleo has published a second patch.[12] Both CVEs have also been added to CISAs Known Exploited Vulnerabilities (KEV) Catalog.[13,14]

The Cal-CSIC recommends immediately updating to the latest Harmony, VLTrader, and LexiCom version (5.8.0.24). Additionally, "Cleo advises those who cannot immediately upgrade to disable the Autorun feature by going into the System Options and clearing out the Autorun directory (this will not block incoming attacks but will reduce the attack surface)."[15]

For further information on applying updates please refer to Cleo Solution Center.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This advisory is based on information obtained from trusted sources, such as Cleo, the National Vulnerability Database, and CISA. Additional information was obtained from opensource cybersecurity news websites.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] National Vulnerability Database; "CVE-2024-50623 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-50623; accessed 18 December 2024

[2] National Vulnerability Database; "CVE-2024-55956 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-55956; accessed 18 December 2024

[3] Cybersecurity and Infrastructure Security Agency; "Known Exploited Vulnerabilities Catalog" https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-50623&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 18 December 2024

[4] Cybersecurity and Infrastructure Security Agency; "Known Exploited Vulnerabilities Catalog" https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-55956&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 18 December 2024

[5] Huntress; “Threat Advisory: Oh No Cleo! Cleo Software Actively Being Exploited in the Wild” https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild; accessed 18 December 2024

[6] Security Week; " CVE Assigned to Cleo Vulnerability as Cl0p Ransomware Group Takes Credit for Exploitation” https://www.securityweek.com/cve-assigned-to-cleo-vulnerability-as-cl0p-ransomware-group-takes-credit-for-exploitation/; accessed 18 December 2024

[7] Cleo Solution Center; “Cleo Product Security Update - CVE-2024-55956” https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956; accessed 18 December 2024

[8] Cybersecurity and Infrastructure Security Agency; “Known Exploited Vulnerabilities Catalog” https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-50623&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 18 December 2024

[9] Cybersecurity and Infrastructure Security Agency; “Known Exploited Vulnerabilities Catalog” https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-55956&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 18 December 2024

[10] Cleo Solution Center; Cleo Product Security Advisory - CVE-2024-50623” https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623; accessed 18 December 2024

[11] Huntress; “Threat Advisory: Oh No Cleo! Cleo Software Actively Being Exploited in the Wild” https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild; accessed 18 December 2024

[12] Cleo Solution Center; “Cleo Product Security Update - CVE-2024-55956” https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956; accessed 18 December 2024

[13] Cybersecurity and Infrastructure Security Agency; “Known Exploited Vulnerabilities Catalog” https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-50623&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 18 December 2024

[14] Cybersecurity and Infrastructure Security Agency; “Known Exploited Vulnerabilities Catalog” https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-55956&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 18 December 2024

[15] BleepingComputer; “Cleo patches critical zero-day exploited in data theft attacks” https://www.bleepingcomputer.com/news/security/cleo-patches-critical-zero-day-exploited-in-data-theft-attacks/; accessed 18 December 2024