An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2412100155

NCSC Advisory

Critical Vulnerabilities in Cleo Harmomy, LexiCom, VLTrader (CVSSv3: 8.8)

10th, December 2024

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Description

CVE ID: CVE-2024-50623

Published: 2024-10-27

Vendor: Cleo

Product: Harmomy, LexiCom, VLTrader

CVSS3.0 Score[1]: 8.8

Products Affected

Product	Version
Harmomy	5.8.0.21 and below
VLTrader	5.8.0.21 and below
LexiCom	5.8.0.21 and below

Impact

In Cleo Harmony up to 5.8.0.21, VLTrader up to 5.8.0.21, and LexiCom up tp 5.8.0.21, there is an unrestricted file upload and download that could lead to remote code execution.

Common Weakness Enumeration (CWE)[2]: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

CISA’s Known Exploited Vulnerability Catalog does not show this vulnerability as exploited at the time of writing. However a known CyberSecurity firm based in the US with a widely reputable Threat Intelligence capabilty, Huntress, have outlined that they have identified this vulnerability as being exploited in the wild. (Please note these findings have not been verfied by the NCSC). Their report is linked below.

[1] https://www.first.org/cvss/v3.0/specification-document

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommedations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cleo.

- https://nvd.nist.gov/vuln/detail/CVE-2024-50623
- https://www.cve.org/CVERecord?id=CVE-2024-50623
- https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory
- https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Advisory-December-9-2024
- https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild