

CVE-2024-50623

Cleo Multiple Products Unrestricted File Upload Vulnerability

Exigent

CISA KEV since Dec 13, 2024

Actively exploited

Ransomware use known

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

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.986 99.92nd percentile · FIRST	CISA DEADLINE Jan 3, 2025 KEV since 2024 · listed over a year
--	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.986 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
harmony	< 5.8.0.21	5.8.0.21	NVD
lexicom	< 5.8.0.21	5.8.0.21	NVD
vltrader	< 5.8.0.21	5.8.0.21	NVD

Sources

Vendor guidance github.com/advisories/GHSA-8j74-v9cr-x39h**Additional guidance** support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory**support.cleo.com** support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update**NVD** nvd.nist.gov/vuln/detail/CVE-2024-50623**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2024-45217**Current data** evulnable.com/vulnerability-management/cve/CVE-2024-50623

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.