Exploitation of Cleo File Transfer Software Vulnerabilities

Overview

Attackers are actively exploiting vulnerabilities in Cleo's file transfer software products—Harmony, VLTrader, and LexiCom. Attackers could gain unauthorized access, execute malicious files, and compromise systems. The vulnerabilities include CVE-2024-50623, an unrestricted file upload and download flaw, and an unauthenticated host zero-day that leads to remote code execution.

Vulnerability Breakdown

- **CVE-2024-50623**
    - Affected Products - Harmony, VLTrader, and LexiCom (versions up to 5.8.0.23)
    - Description - Unrestricted file upload and download vulnerability allowing attackers to install malicious backdoor code.
    - Status - Patch released in October 2024 (v5.8.0.21) was ineffective.
- **Unauthenticated Host Zero-Day** (CVE pending)
    - Affected Products - Harmony, VLTrader, and LexiCom (all versions, including 5.8.0.21)
    - Description - Exploitation through default settings of the Autorun directory, allowing attackers to execute arbitrary bash or PowerShell commands.
    - Status – No patch, just mitigations.

Exploitation of these vulnerabilities can lead to unauthorized access to Cleo file transfer servers, allowing attackers to execute arbitrary commands and deploy malicious backdoors. This could result in data theft and unauthorized changes to systems. Users should patch immediately.

Aspire Protects

- **Patch –** Cleo released a patch in October 2024 (v5.8.0.21) for CVE-2024-50623, but it does not fully resolve the issue. A new patch is being developed, along with a fix for the unauthenticated host zero-day affecting all versions of Harmony, VLTrader, and LexiCom. Organizations should implement interim mitigations until effective patches are available.
- **Mitigations – CVE-2024-50623**
    - Move internet-exposed Cleo systems behind a firewall to limit access.
    - Use endpoint detection and response (EDR) tools to monitor for unauthorized changes.
    - Disabling Cleo's Autorun Directory—which automatically processes command files—can help block the later stages of the attack chain.

  - Apply Cleo's recommended scripts to identify and quarantine malicious files.

- **Unauthenticated Host Zero-Day**
  - Disable the Autorun feature via the interface or provided scripts if not in use.
  - Change the default Autorun directory to a custom name.
  - Block known malicious IP addresses at the network or firewall level.
  - Implement configuration changes to restrict access and monitor for suspicious activity.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Attackers are leveraging file upload vulnerabilities to gain entry.

Execution

- Command and Scripting Interpreter (T1059) – Use of bash/PowerShell commands via Autorun exploitation.

Credential Access

- Account Discovery (T1087) – Enumeration of Active Directory assets using Nltest.

Defense Evasion

- Indicator Removal on Host (T1070) – Deletion of files post-exploitation to maintain stealth.

IoCs

IP Addresses

- 176[.]123[.]5[.]126
- 5[.]149[.]249[.]226
- 185[.]181[.]230[.]103
- 209[.]127[.]12[.]38
- 181[.]214[.]147[.]164
- 192[.]119[.]99[.]42

Malicious Files

- 60282967-dc91-40ef-a34c-38e992509c2c.xml
- healthchecktemplate.txt or healthcheck.txt

Targeted Industries

Industries potentially affected by the vulnerabilities due to the use of file transfer systems:

- Healthcare
- Manufacturing
- Government

- Legal
- Finance

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cleo Software Actively Being Exploited in the Wild | Huntress

Cleo Product Security Advisory - CVE-2024-50623 – Cleo

Cleo Product Security Advisory (CVE Pending) – Cleo

Widespread exploitation of Cleo file transfer software (CVE-2024-50623) | Rapid7 Blog