

Posted Date: 2025/11/12

[Vulnerability Alert] CISA Added 2 Known Exploited Vulnerabilities to KEV Catalog (2025/11/03-2025/11/09) (CVE-2025-48703) (CVE-2025-11371)

- Subject: [Vulnerability Alert] CISA Added 2 Known Exploited Vulnerabilities to KEV Catalog (2025/11/03-2025/11/09) (CVE-2025-48703) (CVE-2025-11371)
- Content:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202511-00000005
 - [CVE-2025-48703] CWP Control Web Panel OS Command Injection Vulnerability (CVSS v3.1: 9.0)
 - [Exploited by Ransomware: Unknown] CWP (also known as Control Web Panel or CentOS Web Panel) has an Operating System Command Injection vulnerability that allows unauthenticated remote code execution via the `t_total` parameter in the file manager's `changePerm` request.
 - [CVE-2025-11371] Gladinet CentreStack and Triofox Files or Directories Accessible to External Parties Vulnerability (CVSS v3.1: 7.5)
 - [Exploited by Ransomware: Unknown] The default installation and configuration of Gladinet CentreStack and TrioFox allows unauthenticated attackers to access local files or directories.
- Affected Platforms:
 - [CVE-2025-48703] CentOS Web Panel versions prior to 0.9.8.1205 (exclusive)
 - [CVE-2025-11371] CentreStack and TrioFox versions up to and including 16.7.10368.56560
- Recommended Measures:
 - [CVE-2025-48703] Upgrade the corresponding product to CentOS Web Panel version 0.9.8.1205 (inclusive) or later
 - [CVE-2025-11371] Upgrade the corresponding product to CentreStack and TrioFox versions later than 16.7.10368.56560 (exclusive)

Computer and Communications Center
Network Systems Group

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251112_02

Last update: **2025/11/12 15:31**

