Health-ISAC®
Collaborating for Resilience in Health
SHARING SINCE 2010

VULNERABILITY BULLETINS

Active Exploitation of Gladinet CentreStack and TrioFox Products (CVE-2025-11371)

TLP:WHITE

Oct 10, 2025

On October 9, 2025, Huntress disclosed the observance of active, in-the-wild exploitation of CVE-2025-11371, an unauthenticated local file inclusion (LFI) vulnerability impacting Gladinet CentreStack and TrioFox products. The cybersecurity company has confirmed that three of its customers have been affected so far.

This flaw is currently a zero-day with no official vendor patch, but a strong mitigation is available that organizations should implement immediately. Exploiting this vulnerability allows attackers to retrieve configuration keys, which they then use to achieve remote code execution (RCE) and compromise the server.

Health-ISAC is sharing this to increase situational awareness and encourage organizations to assess their level of risk to the vulnerability and exploitation activity.

Gladinet CentreStack and TrioFox are enterprise solutions designed to modernize file access and sharing, enabling remote teams to securely access files without relying on complex VPNs. CentreStack is typically aimed at Managed Service Providers (MSPs) and small businesses, often offering multi-tenant or cloud-based deployment. TrioFox, conversely, is tailored for large enterprises, providing a secure gateway for on-premises file servers, allowing users to access files via HTTPS streaming while retaining data control. Due to their role as essential file access and remote work infrastructure, the compromise of these platforms poses a severe risk.

The vulnerability, tracked as CVE-2025-11371, is an unauthenticated local file inclusion (LFI) flaw found in the default installation and configuration of both CentreStack and TrioFox. This bug allows an attacker to manipulate file paths in requests to the device, forcing the application to read and disclose sensitive system files that it should not expose. This vulnerability impacts all versions of the software prior to and including the latest available version, 16.7.10368.56560.

Exploiting this security flaw is a critical step in a two-stage attack chain. Threat actors use CVE-2025-11371 to retrieve the sensitive machineKey value from the application's Web.config file. Once the attacker possesses this key, they can then leverage a previously addressed but now-re-weaponized ViewState deserialization vulnerability (CVE-2025-30406). By forging a malicious ViewState payload signed with the stolen key, the attacker bypasses security checks and achieves remote code execution (RCE) on the underlying infrastructure hosting the Gladinet product.

The security implications of remote code execution attacks on a CentreStack or TrioFox server have the potential to be immediate and devastating. Since these platforms manage access to corporate file shares, a compromise grants the attacker high-level access to the organization's data. Previous attacks observed by Huntress exploiting CVE-2025-30406 were launched to deploy malicious executable files, install remote access tools, and conduct lateral movement across victim networks.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Implementing the temporary workaround by disabling the temp handler within the Web.config file for UploadDownloadProxy located at:
    - C:\Program Files (x86)\Gladinet Cloud Enterprise\UploadDownloadProxy\Web.config
- Ensuring that access to the CentreStack/TrioFox management interface is strictly controlled and not unnecessarily exposed to the public internet
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	thehackernews, hhs, huntress, helpnetsecurity

Alert ID 78f8be90

View Alert

Share Feedback

was this helpful? 👍 | 👎

Tags TrioFox, CentreStack, Gladinet, CVE-2025-30406, CVE-2025-11371

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps.

Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.