Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-11371: Critical Gladinet Flaw Actively Exploited in the Wild

Date of Publication	Date of Publication	Admiralty Code	TA Number
October 13, 2025	November 4, 2025	A1	TA2025314

Summary

First Seen: September 27, 2025
Affected Product: Gladinet CentreStack and Triofox
Impact: CVE-2025-11371 is an unauthenticated Local File Inclusion (LFI) vulnerability in Gladinet's CentreStack and TrioFox platforms, affecting versions up to 16.7.10368.56560. The flaw allows remote attackers to read sensitive files such as Web.config, exposing the machine key used for ASP.NET ViewState validation. This key can then be leveraged with CVE-2025-30406 to achieve remote code execution. The vulnerability had been actively exploited since late September 2025 but was patched in version 16.10.10408.56683. All users are strongly advised to upgrade to the patched release to mitigate risk.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-11371	Gladinet CentreStack and Triofox Files or Directories Accessible to External Parties Vulnerability	Gladinet CentreStack and Triofox	✓	✓	✓
CVE-2025-30406	Gladinet CentreStack and Triofox Use of Hard-coded Cryptographic Key Vulnerability	Gladinet CentreStack and Triofox	✓	✓	✓

Vulnerability Details

#1

CVE-2025-11371 is an unauthenticated Local File Inclusion (LFI) vulnerability affecting Gladinet CentreStack and TrioFox (file sharing/ remote access platforms) in default configurations up to version 16.7.10368.56560. The flaw allows an attacker with network access to read arbitrary files on the target system, including sensitive configuration files such as Web.config. The vulnerability has been actively exploited in the wild since September 27, 2025, when a CentreStack instance running a version already patched against CVE-2025-30406 was compromised through a newly discovered LFI route.

#2

Through this flaw, attackers were able to extract the machine key from Web.config, a crucial secret used in ASP.NET ViewState validation, enabling them to craft malicious ViewState payloads. These forged payloads can then exploit CVE-2025-30406, a deserialization vulnerability tied to predictable machine keys, to achieve remote code execution (RCE). While the LFI by itself primarily threatens confidentiality, its ability to be chained to an RCE path makes it far more severe.

#3

CVE-2025-11371 carries a CVSS score around 6.1, reflecting the moderate inherent risk of file disclosure alone. However, the overall impact escalates sharply when the disclosed machine key is weaponized through the earlier ViewState exploit. Gladinet released a patch in mid-October 2025 (version 16.10.10408.56683) addressing this issue and mitigating the attack chain. All CentreStack and TrioFox deployments running earlier builds should be updated immediately, and any system previously exposed should have its machine Key and credentials rotated to prevent post-compromise persistence.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-11371	Gladinet CentreStack and Triofox: All versions prior to and including 16.7.10368.56560	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:* cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*	CWE-552
CVE-2025-30406	Gladinet CentreStack versions prior to 16.4.10315.56368 Gladinet Triofox versions prior to 16.4.10317.56372	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:* cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*	CWE-321

Recommendations

Disable the 'temp' handler in Web.config: Disable the "temp" handler in the UploadDownloadProxy section of the Web.config file in Gladinet CentreStack and TrioFox installations. This involves removing or commenting out the line referencing Gladinet.Cloud.Proxy.TempHandler in Web.config. This step blocks unauthenticated access to the vulnerable file inclusion endpoint, preventing exploitation of the Local File Inclusion (LFI) flaw.

Rotate ASP.NET Machine Keys: Since the LFI flaw is exploited to steal the machine key, the key must be immediately rotated, even if the system was previously patched for CVE-2025-30406. Rotating the key invalidates any malicious ViewState payloads an attacker might craft and breaks the final stage of the RCE attack chain, requiring an IIS reset after the change.

Implement Network Segmentation/Access Controls: Restrict network access to the CentreStack/Triofox web services, particularly the affected UploadDownloadProxy endpoint, to trusted users or internal networks only. Reducing external exposure minimizes the attack surface, making it much harder for unauthenticated remote attackers to initiate the LFI and subsequent RCE exploit.

Monitor and Audit System Logs: Actively monitor server logs for suspicious read requests targeting sensitive configuration files like Web.config or for unusual, irregular base64-encoded ViewState payloads.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0006 Credential Access	TA0042 Resource Development
TA0007 Discovery	TA0004 Privilege Escalation	T1552.001 Credentials In Files	T1552 Unsecured Credentials
T1588.006 Vulnerabilities	T1588.005 Exploits	T1588 Obtain Capabilities	T1083 File and Directory Discovery
T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation

Patch Details

CVE-2025-11371: Upgrade Gladinet CentreStack and Triofox to 16.10.10408.56683 or later
CVE-2025-30406: Fixed in the following versions:
Windows: 16.4.10315.56368
macOS: 15.12.434

Link: https://www.centrestack.com/p/gce_latest_release.html

References

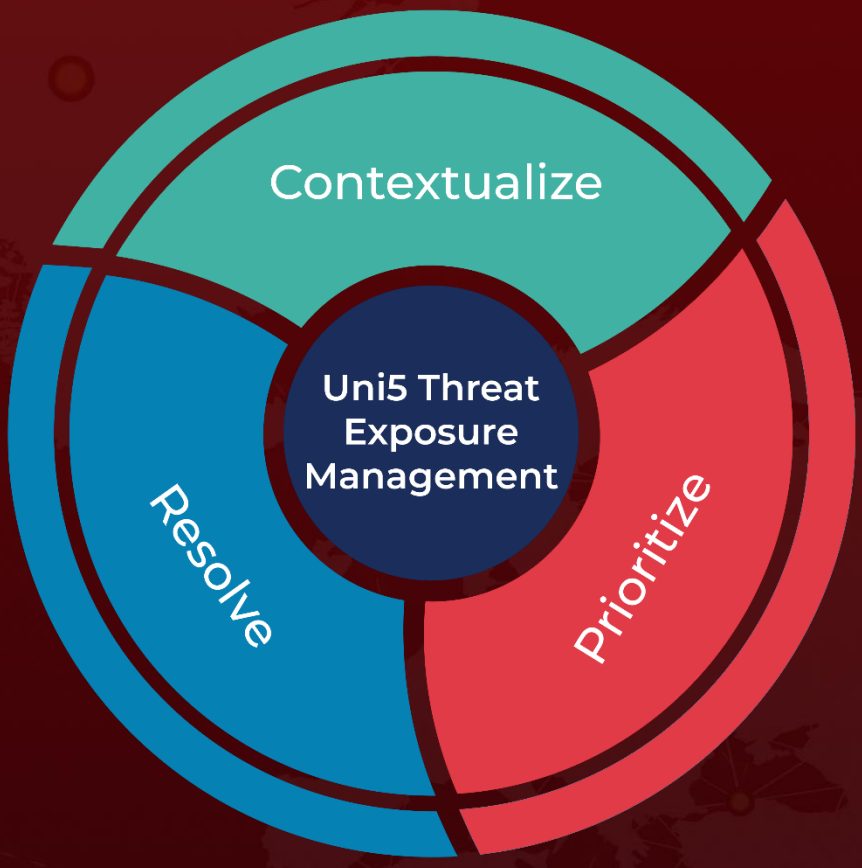
https://www.huntress.com/blog/gladinet-centrestack-triofox-local-file-inclusion-flaw

https://hivepro.com/threat-advisory/centrestack-rce-vulnerability-actively-exploited-in-the-wild/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 13, 2025 . 10:30 AM

More at www.hivepro.com