Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CentreStack RCE Vulnerability Actively Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
April 10, 2025	A1	TA2025109

Summary

First Seen: March 2025
Affected Products: Gladinet CentreStack
Affected Platforms: Windows, macOS
Impact: A critical zero-day vulnerability in Gladinet CentreStack's secure file-sharing software, CVE-2025-30406 has been exploited in the wild since March, putting countless storage servers at risk. The flaw involves a hard-coded cryptographic key that attackers can leverage to gain remote code execution, potentially allowing them full control over affected systems. Now that a patch has been released, it's vital for all CentreStack users to upgrade immediately. Delaying the update leaves systems exposed to ongoing exploitation, making swift action essential to protect sensitive data and infrastructure.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-30406	Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability	Gladinet CentreStack	✓	✓	✓

Vulnerability Details

#1

A critical zero-day vulnerability, tracked as CVE-2025-30406, has been actively exploited since March in Gladinet CentreStack a self-hosted, enterprise-grade file-sharing platform that provides secure, cloud-like access to internal file servers. Commonly used by businesses for remote access, file synchronization, and team collaboration, CentreStack allows organizations to maintain data control without relying on services like Dropbox or Google Drive.

#2 The vulnerability stems from insecure handling of cryptographic keys, specifically the machineKey stored in the IIS web.config file. If this key is hardcoded or weakly protected, attackers can obtain or guess it to forge ASP.NET ViewState payloads that bypass integrity checks. In vulnerable configurations, this can lead to remote code execution (RCE) on the server allowing attackers to gain full control.

#3 Given that the flaw is already being actively exploited in the wild, organizations are strongly urged to apply the latest patch released by Gladinet. For those unable to upgrade immediately, a critical temporary mitigation is to rotate the machineKey values to reduce the risk of compromise.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-30406	Gladinet CentreStack through 16.1.10296.56315	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:*	CWE-321

Recommendations

Upgrade Immediately: Upgrade to the Latest Patched Version (Build 16.4.10315.56368). Gladinet has released a security patch that addresses the vulnerability by automatically generating a unique machineKey for every installation. Upgrading to this version is the most effective way to protect your system from remote code execution attacks linked to CVE-2025-30406.

Workaround: If updating to the patched version isn't possible right away, make sure to manually generate a strong, unique machineKey and apply it to your web.config file. This helps block attackers from crafting malicious ViewState payloads. Follow Gladinet's official guidance to safely rotate the key and reduce your risk.

Monitor Suspicious Activities: Watch your web server logs for anything unusual especially weird patterns related to ViewState. Turn on auditing for important config files and stay alert for signs of tampering or unexpected remote commands. Catching these early can help stop an attack in its tracks.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0006 Credential Access
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1552 Unsecured Credentials	T1552.004 Private Keys		

Patch Details

Gladinet has rolled out patches for the critical CVE-2025-30406 vulnerability in the following versions:
Windows: 16.4.10315.56368
macOS: 15.12.434

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

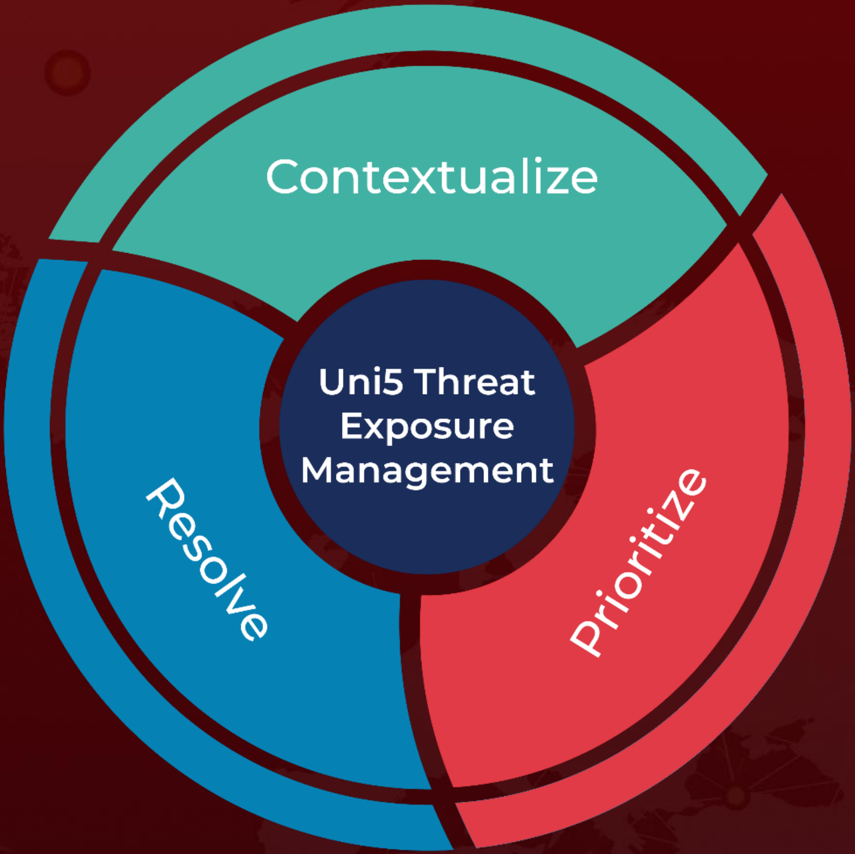
References

https://gladinetsupport.s3.us-east-1.amazonaws.com/gladinet/securityadvisory-cve-2005.pdf

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

April 10, 2025 • 6:20 AM

More at www.hivepro.com