Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-12480: Triofox Exploit Turns Trusted Access Into a Security Nightmare

Date of Publication	Admiralty Code	TA Number
November 14, 2025	A1	TA2025346

Summary

Attack Commenced: August 2025
Threat Actor: UNC6485
Affected Product: Gladinet Triofox
Impact: The Threat actor group UNC6485 is exploiting CVE-2025-12480, a major security flaw in Gladinet's Triofox software, which allows them to break in without logging in and take full control of affected systems. They exploit the flaw to create fake admin accounts, execute malicious code, and install remote-access tools such as Zoho Assist and AnyDesk to control networks. Organizations using older Triofox versions are at serious risk of data theft and system compromise. This attack follows another recent vulnerability in Gladinet's products, showing continued targeting of remote-access and file-sharing platforms.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-12480	Gladinet Triofox Improper Access Control Vulnerability	Gladinet Triofox	✗	✓	✓

Vulnerability Details

#1 A Threat Actor group identified as UNC6485 has exploited a critical security flaw in Gladinet's Triofox platform, tracked as CVE-2025-12480. The vulnerability allows attackers to bypass authentication, gain administrative access, and execute code with full system privileges. Active exploitation began on August 24, 2025.

#2 The flaw results from an access control weakness that grants admin access when a request appears to come from localhost. Attackers can falsify this value through the HTTP Host or Referer header, bypassing authentication. Systems without a properly configured TrustedHostIp setting remain exposed to unauthenticated access.

#3 Using this method, UNC6485 accessed Triofox's AdminDatabase.aspx setup page, created a new administrator account named Cluster Admin, and uploaded a malicious script. They reconfigured the platform's antivirus feature to run this script, which then executed with system-level privileges.

#4 The script downloaded a Zoho UEMS installer used to deploy Zoho Assist and AnyDesk, enabling remote access and lateral movement. The attackers also used Plink and PuTTY to create SSH tunnels and forward traffic to the host's RDP port, establishing encrypted connections to their command-and-control servers.

#5 Organizations running Triofox version 16.4.10317.56372 or earlier are at immediate risk of unauthorized access, remote tool deployment, and potential network compromise. In the previous month, another zero-day vulnerability was exploited, **CVE-2025-11371**, in both Gladinet CentreStack and Triofox, which allowed unauthenticated access to system files.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-12480	Gladinet Triofox version 16.4.10317.56372	cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*	CWE-284

Recommendations

Upgrade Triofox Software Immediately: Apply the latest Triofox update (version 16.7.10368.56560 or newer) across all deployments. This release addresses the exploited CVE-2025-12480 vulnerability that allows attackers to gain full system control. Delayed patching leaves servers exposed to attacks by UNC6485.

Audit All Administrative Accounts: Perform a detailed review of all administrator accounts within Triofox and the connected domain. Pay close attention to suspicious accounts such as "Cluster Admin" or any accounts created after August 2025. Remove unauthorized entries and reset passwords for legitimate users.

Monitor Process and Command Activity: Track system processes for instances of GladinetCloudMonitor.exe launching cmd.exe, PowerShell, or other command-line tools. Such activity is a strong indicator of command execution attempts through the compromised antivirus configuration.

Restrict Administrative Access Points: Update the web.config file to define the TrustedHostIP parameter. Restrict access to administrative interfaces to trusted internal IPs only. This prevents attackers from exploiting the "localhost" bypass flaw through spoofed headers.

Adopt Zero Trust Authentication: Apply Zero Trust principles to Triofox access control. Require authentication and authorization at the application layer, regardless of network location or IP origin. This prevents misuse of internal-trust assumptions.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1562 Impair Defenses
T1190 Exploit Public-Facing Application	T1055 Process Injection	T1136 Create Account	T1136.001 Local Account
T1569 System Services	T1569.002 Service Execution	T1219 Remote Access Tools	T1219.002 Remote Desktop Software
T1572 Protocol Tunneling	T1098 Account Manipulation	T1105 Ingress Tool Transfer	T1087 Account Discovery
T1036 Masquerading	T1036.005 Match Legitimate Resource Name or Location	T1027 Obfuscated Files or Information	T1562.001 Disable or Modify Tools
T1068 Exploitation for Privilege Escalation			

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxp[:]//84[.]200[.]80[.]252/SAgentInstaller_16[.]7[.]10368[.]56560[.]zip
File Path	C:\Windows\appcompat\SAgentInstaller_16.7.10368.56560.exe, C:\Windows\temp\sihosts.exe, C:\Windows\temp\silcon.exe, C:\Windows\temp\file.exe, C:\triofox\centre_report.bat
SHA256	43c455274d41e58132be7f66139566a941190ceba46082eb2ad7a6a261bfd63f, 50479953865b30775056441b10fdcb984126ba4f98af4f64756902a807b453e7, 16cbe40fb24ce2d422afddb5a90a5801ced32ef52c22c2fc77b25a90837f28ad, ac7f226bdf1c6750afa6a03da2b483eee2ef02cd9c2d6af71ea7c6a9a4eace2f
IPv4	85[.]239[.]63[.]37, 65[.]109[.]204[.]197, 84[.]200[.]80[.]252, 216[.]107[.]136[.]46

Patch Details

The vulnerability has been patched in Triofox version 16.7.10368.56560, requiring immediate upgrade and a comprehensive security audit of affected systems.

Link:
https://access.triofox.com/releases_history/

References

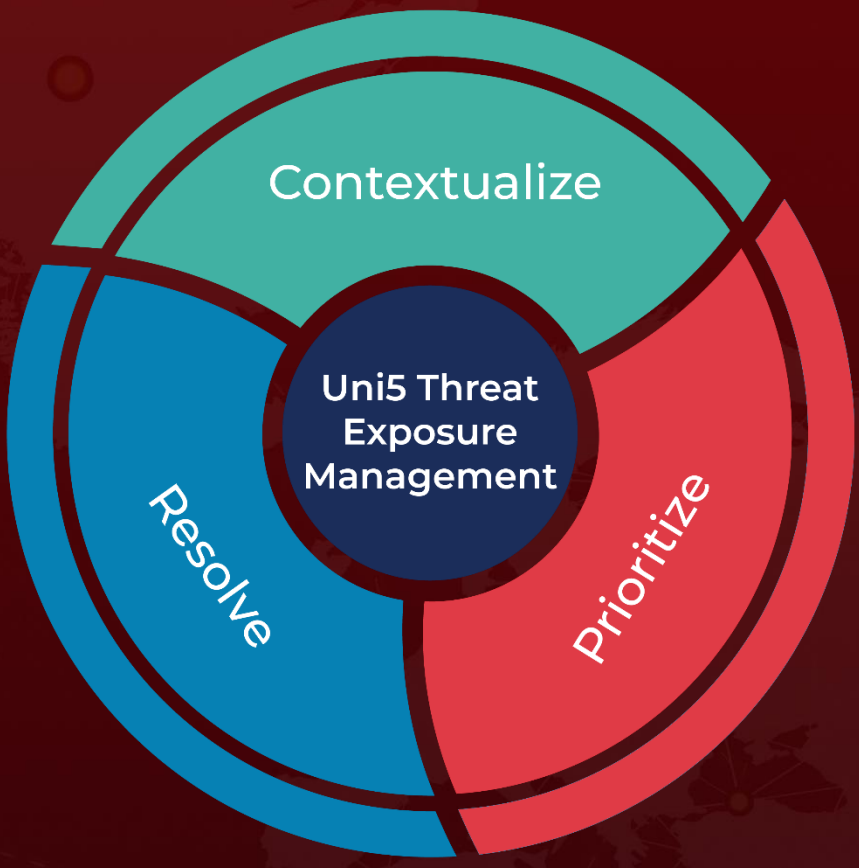
https://cloud.google.com/blog/topics/threat-intelligence/triofox-vulnerability-cve-2025-12480

https://hivepro.com/threat-advisory/critical-gladinet-flaw-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

November 14, 2025 . 04:00 AM

More at www.hivepro.com