مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Gladinet Triofox

Tracking #:432317988

Date:11-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability in Gladinet's Triofox file-sharing and remote access platform is being actively exploited to gain unauthorized administrative access and execute code with SYSTEM-level privileges. The flaw allows remote attackers to bypass authentication, create new administrative accounts, and deploy additional payloads.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-12480**
- CVSS v2 Base Score: 9.4 (Critical)
- The vulnerability results from **improper access control** in the Triofox web interface. By spoofing the HTTP Host header to localhost, attackers can access restricted setup pages (e.g., AdminDatabase.aspx), create a new admin account, and abuse the antivirus configuration feature to execute a malicious script as SYSTEM.
- Observed exploitation involved PowerShell downloads, installation of remote access tools, and RDP tunneling through encrypted SSH channels.

Exploitation activity included:

- Creation of a new admin account ("Cluster Admin")
- Execution of PowerShell commands to download payloads (e.g., from 84.200.80[.]252)
- Deployment of remote access tools (e.g., Zoho Assist, AnyDesk)
- RDP tunneling via PuTTY/Plink over port 433

Indicators of Compromise (IOCs)
Attached in Excel File

Affected Versions

- Triofox 16.4.10317.56372 and earlier

Fixed Versions

- Triofox 16.7.10368.56560 and later

RECOMMENDATIONS:

- Apply the latest software updates and security patches.
- Review administrative accounts and remove any unauthorized access.
- Ensure security controls prevent unauthorized execution of scripts or binaries.
- Monitor network and endpoint activity for suspicious behavior.
- Conduct regular security audits and threat hunting to detect anomalies.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.tenable.com/cve/CVE-2025-12480