



# Teclib GLPI Remote Code Execution Vulnerability

## Critical vulnerability in a third party library module

<https://github.com/glpi-project/glpi/releases>

CVEs: [CVE-2022-35914](#)

A vulnerability is observed in the 3rd-party HTMLAWED module for GLPI through 10.0.2 which allows PHP code injection.

### Background

GLPI (Gestionnaire Libre de Parc Informatique) is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. A remote unauthenticated attacker could exploit this vulnerability (CVE-2022-35914) by sending a crafted request to the target server. Successful exploitation could result in arbitrary code execution in the security context of the web server process which could impact confidentiality, integrity and availability of the system.

### Announced

September 14, 2022: GLPI releases version 10.0.3 with a fix.

<https://glpi-project.org/fr/glpi-10-0-3-disponible/>

March 07, 2023: CISA adds CVE-2022-35914 to its known exploited catalog

### Latest Developments

March 13, 2023: FortiGuard labs is seeing active exploitation attempts to exploit the flaw CVE-2022-35914 and recommends admins to update the GLPI to version 10.0.3 or above.

## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

### Reconnaissance

#### Lure



FortiDeceptor

v3.3+

#### Decoy VM



FortiDeceptor

v3.3+

### Weaponization

### Delivery

### Exploitation

#### IPS

Detects and blocks attempts to exploit vulnerability in the htmlawed module for GLPI (CVE-2022-35914)



FortiGate

DB 22.495



FortiSASE

DB 22.495



FortiNDR

DB 22.495



FortiADC

DB 22.495



FortiProxy

DB 22.495

#### Web App Security

Detects and blocks attempts to exploit vulnerability in the htmlawed module for GLPI (CVE-2022-35914)



FortiWeb

DB 0.00345



FortiADC

DB 1.00042

#### Application Firewall

Detects and blocks attempts to exploit vulnerability in the htmlawed module for GLPI (CVE-2022-35914)



FortiClient

DB 22.495

### Installation

### C2

### Action

## DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

#### Outbreak Detection



FortiAnalyzer

DB 1.00093

#### Threat Hunting



FortiAnalyzer

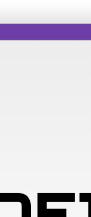
v6.4+



FortiSIEM

v6.6+

#### Content Update



FortiSIEM

DB 313

## RESPOND

Develop containment techniques to mitigate impacts of security events:

#### Automated Response

Services that can automatically respond to this outbreak.



FortiXDR

#### Assisted Response Services



FortiAnalyzer

v6.4+



FortiRecon

v6.6+



FortiDAST

### Content Update

### Readiness

### Response

### FortiRecon

### FortiDAST

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

#### InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.



FortiAnalyzer

DB 22.495

#### InfoSec Services

## IDENTIFY

Identify processes and assets that need protection:

#### Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.



FortiAnalyzer

v6.4+



FortiRecon

v6.6+



FortiDAST

### Attack Surface Monitoring (Inside & Outside)

### Readiness

## Additional Resources

### The Hacker News

<https://thehackernews.com/2023/03/cisas-key-catalog-updated-with-3-new.html>

### LeMagIT

<https://www.lemagit.fr/actualites/252529534/2022-petite-annee-sur-le-front-des-vulnerabilites>

### FortiGuard Threat Signal

<https://www.fortiguard.com/threat-signal-report/5052/>

Learn more about [FortiGuard Outbreak Alerts](#)

