Open Redirect - OrigemControle - listarTodos() & listarId_Nome() - Unvalidated $_GET['nextPage']

Moderate **nilsonLazarin** published **GHSA-jvmq-528w-q4xp** 4 days ago

Package

No package listed

Affected versions

<=3.6.8

Patched versions

3.6.9

Description

Summary

An Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with:

- metodo=listarTodos & listarId_Nome
- nomeClasse=OrigemControle

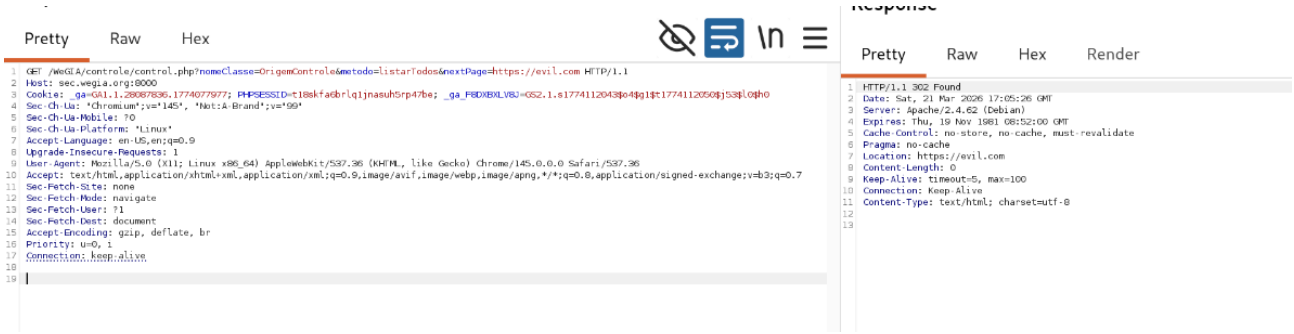
The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain.

PoC

Navigate to the following URL:

```
GET /WeGIA/controle/control.php?
nomeClasse=OrigemControle&metodo=listarTodos&nextPage=https://evil.com HTTP/1.1
Host: sec.wegia.org:8000
```

```
GET /WeGIA/controle/control.php?
nomeClasse=OrigemControle&metodo=listarId_Nome&nextPage=https://evil.com HTTP/1.1
Host: sec.wegia.org:8000
```



Impact

It can be weaponized for phishing by sending a crafted link to an admin: the victim sees a legitimate-looking success message on the attacker's site after clicking. It allows to:

- Redirect users to phishing pages designed to steal credentials.
- Redirect users to malicious sites hosting malware or dangerous content.
- Perform social engineering attacks using trusted URLs from the WeGIA domain.
- Potentially interfere with authentication or session-handling flows.
- Damage user trust in the WeGIA platform.

Severity

Moderate 5.1 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	Active

Vulnerable System Impact Metrics

Confidentiality	Low
Integrity	Low
Availability	None

Subsequent System Impact Metrics

Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

CVE ID

CVE-2026-35398

Weaknesses

▶ CWE-601

Credits

dapickle — Reporter

GabrielPintoSouza — Remediation developer