Open Redirect - atualizacao redirection - Unvalidated $_GET['redirect']

Moderate **nilsonLazarin** published **GHSA-7935-g3wg-h55w** 4 days ago

Package

No package listed

Affected versions

<=3.6.8

Patched versions

3.6.9

Description

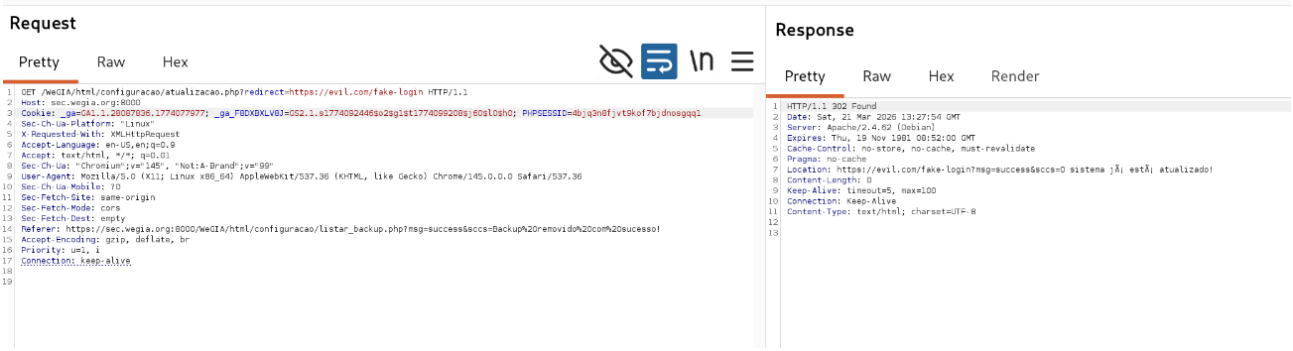
Summary

Open redirect has been found in WeGIA webapp. The redirect parameter is taken directly from $_GET with no URL validation or whitelist check, then used verbatim in a header("Location: ...") call.

PoC with admin

Navigate to the following URL:

```
GET /WeGIA/html/configuracao/atualizacao.php?redirect=https://evil.com/fake-login
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-2026-35474

Weaknesses

▶ CWE-601

Credits

dapickle	Reporter
GabrielPintoSouza	Remediation developer