Unauthenticated SQL Injection on get_socios.php endpoint

Critical **nilsonLazarin** published **GHSA-5qw5-q55h-6qg7** yesterday

Package	Affected versions	Patched versions
php **WeGIA** (Composer)	< 3.3.0	3.3.1

Description

Summary

A Unauthenticated SQL Injection vulnerability was identified in the endpoint `/html/socio/sistema/get_socios.php`, specifically in the query parameter. This issue allows attackers to inject and execute arbitrary SQL statements against the application's underlying database. As a result, it may lead to data exfiltration, authentication bypass, or complete database compromise.

Details

The vulnerable endpoint directly executes user-supplied SQL input from the POST parameter query without proper validation or sanitization. This unsafe use of the mysqli_query() function makes the application susceptible to SQL injection.

```
<?php
    require("../conexao.php");
    $query = $_POST['query'];
    $resultado = mysqli_query($conexao, $query);
    $linhas = mysqli_affected_rows($conexao);
    for($i = 0; $i<$linhas; $i++){
        $tabela["socios"][$i] = mysqli_fetch_array($resultado);
    }
    echo json_encode($tabela);
?>
```

This approach directly processes untrusted user input, enabling malicious actors to craft and execute unauthorized SQL queries.

PoC

Severity

Critical 10.0 / 10

CVSS v4 base metrics

Exploitability Metrics

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

Vulnerable System Impact Metrics

Confidentiality	High
Integrity	High
Availability	High

Subsequent System Impact Metrics

Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2025-46828

Weaknesses

A malicious request such as the one below successfully demonstrates SQL injection by extracting database-related information:

Impact

Exfiltration of confidential data.
Database compromise.

CWE-89

Credits

Finder
GabrielPintoSouza

nmmorette Reporter