Cross-Site Scripting Controle de Contribuição

High **nilsonLazarin** published **GHSA-42rc-rvrx-cmmw** last week

Package

No package listed

Affected versions

<= 3.6.9

Patched versions

3.6.10

Description

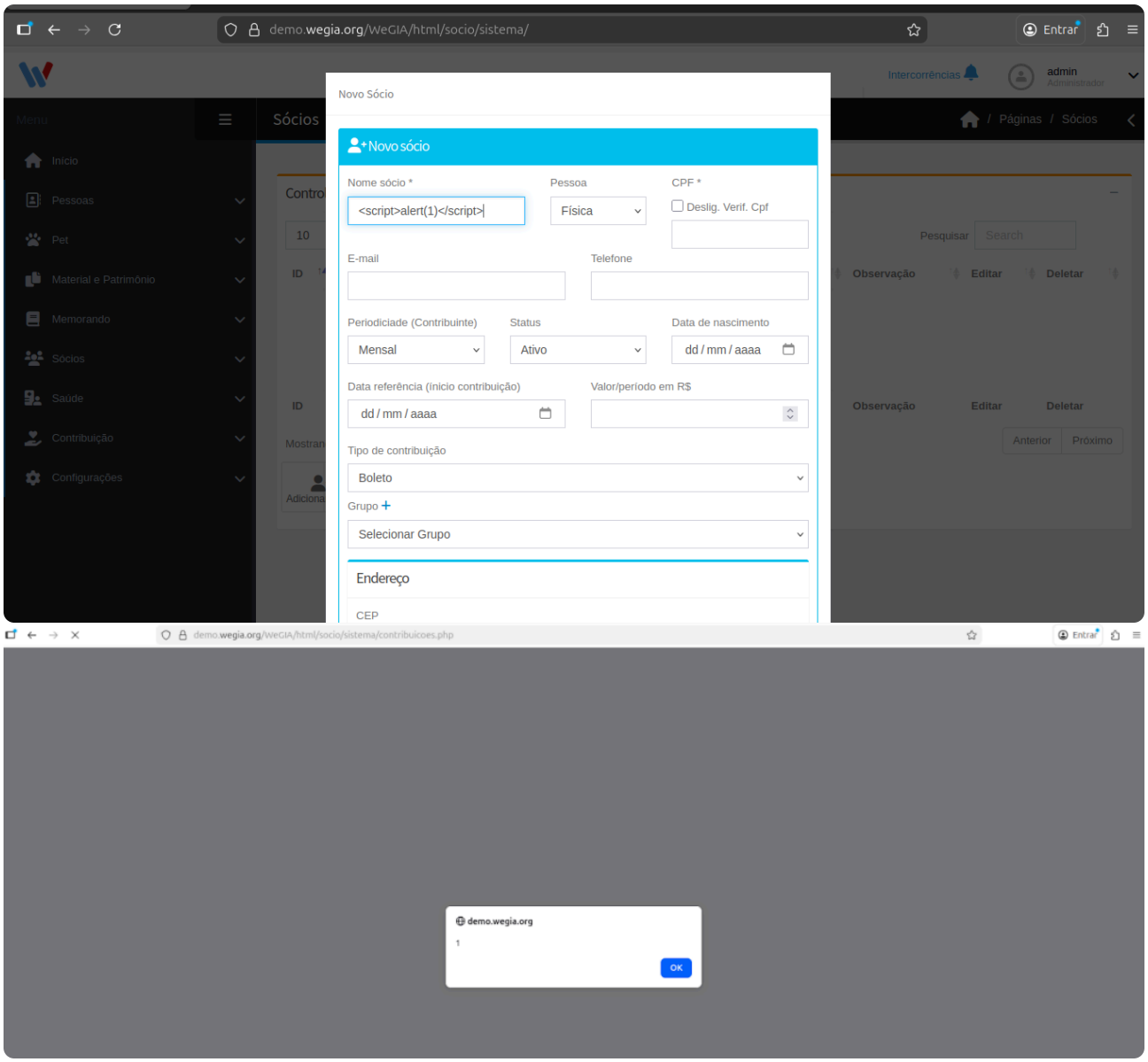
Summary

WeGIA (Web Gerenciador para Instituições Assistenciais) is vulnerable to Cross-Site Scripting (XSS) at the following URLs: https://demo.wegia.org/WeGIA/html/socio/sistema/, https://demo.wegia.org/WEGIA/html/socio/sistema/contribuicoes.php. An attacker can exploit this flaw to execute a malicious payload within the context of the user's browser.

Details

A Stored Cross-Site Scripting (XSS) vulnerability was identified in the 'Member Registration' (Cadastrar Sócio) function. By injecting a payload—such as <script>alert(1)</script>—into the 'Member Name' (Nome Sócio) field, the script is persistently stored in the database. Consequently, the payload is executed whenever a user navigates to the following URL: https://demo.wegia.org/WEGIA/html/socio/sistema/contribuicoes.php.

PoC



Impact

Sensitive Data Capture

Injected JavaScript can manipulate the page's behavior to capture user input. This includes:

Keylogging: The script records every keystroke and exfiltrates the data to an attacker-controlled server.

Credential Harvesting/Phishing: An attacker can perform DOM manipulation to inject fraudulent fields (e.g., "Confirm your password" or "Enter your SSN/CPF") into the legitimate page. Since the user trusts the WeGIA domain, they are likely to provide sensitive information without suspicion.

Severity

High 7.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None

User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVE ID

CVE-2026-40286

Weaknesses

No CWEs

Credits

 **Arthurvel** Reporter

 **GabrielPintoSouza** Remediation developer