Stored XSS in intercorrencia_visualizar.php

Moderate **nilsonLazarin** published **GHSA-r6h8-7vxv-q8pp** last week

Package

No package listed

Affected versions

<= 3.6.8

Patched versions

3.6.10

Description

Summary

A Stored Cross-Site Scripting (XSS) vulnerability allows an authenticated user to inject malicious JavaScript into the Intercorrências notification page, which is executed when user access the the page, enabling session hijacking and account takeover.

Details

The application does not properly sanitize or encode the user name field, which is displayed in system notifications and accepts user-controlled input. An attacker can inject malicious HTML or JavaScript into this field when creating or modifying a user.

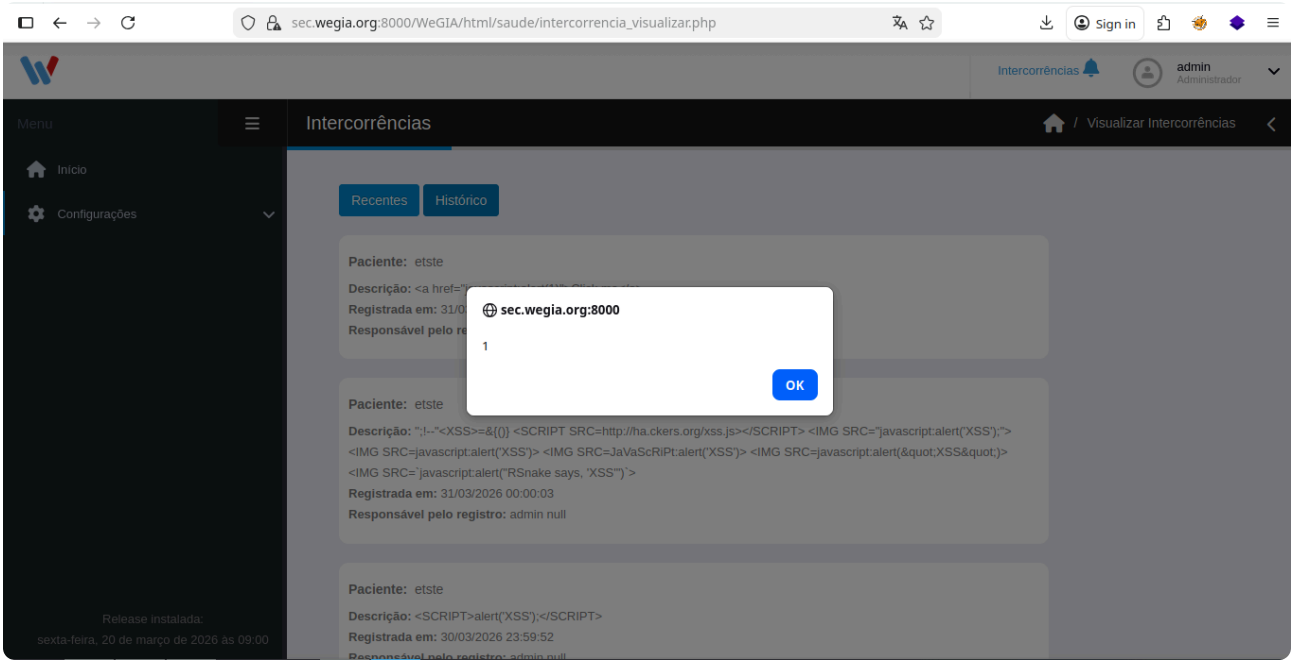
When an “intercorrência” is registered, a notification is generated. Upon clicking this notification, the application renders the user name in the interface without proper escaping, causing any injected code to be executed in the browser.

This behavior demonstrates improper output encoding, resulting in a Stored XSS vulnerability.

PoC

1. Register a patient where the “Name” or "Sobrenome" field contains the following payload: `<img src=1 onerror=alert("XSS")>`
2. Add a "Intercorrência" entry for this user

3. Navigate to the "Intercorrências" notification page and click in "Recentes" and "Histórico. This vulnerability affects the both pages.
4. Observe that the payload is executed in the browser



Impact

This is a Stored XSS vulnerability affecting all users who access the Intercorrências notification page.

An attacker can:

1. Execute arbitrary JavaScript in victims' browsers
2. Steal session cookies
3. Perform actions on behalf of authenticated users
4. Potentially achieve account takeover

Credits

Thiago Escarrone

Severity

Moderate 6.4 / 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	High
Integrity	High
Availability	High

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:H/SI:H/SA:H

CVE ID

CVE-2026-40282

Weaknesses

▶ CWE-79

Credits

ThiagoEscarrone — Reporter

GabrielPintoSouza — Remediation developer