New issue

CVE-2026-6622 #18

Closed

Labels CVE

4m3rr0r opened 3 weeks ago · edited by 4m3rr0r Edits Owner

Description

The application allows users or administrators to input data into the Full Name and Home Address fields without proper sanitization or output encoding.

These values are stored in the database and later rendered in multiple parts of the application, including customer list and edit pages.
Because the application fails to escape user input before rendering it in HTML, attackers can inject malicious JavaScript payloads that execute in the browser of any user viewing the affected page.

Product Information

- Product: BichitroGan ISP Billing System
- Vendor Homepage: https://bichitrogan.com/isp-billing/
- Software Link: https://demo.bichitrogan.com/redirect.html
- Affected Version: 2025.3.20

Affected Endpoints

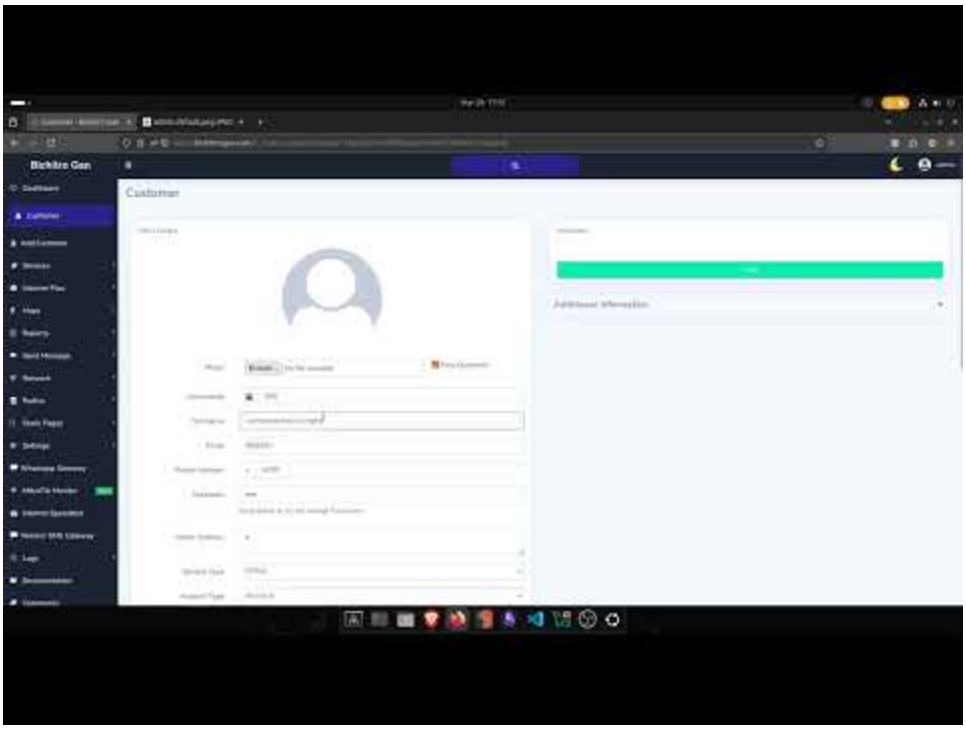
- Customer List: https://demo.bichitrogan.com/?_route=customers/list
- Customer Edit: https://demo.bichitrogan.com/?_route=customers/edit/{id}

Vulnerable Parameters

- fullname
- address (Home Address)

Proof of Concept (PoC)

Watch the video



Steps to Reproduce: 1. Login as a user or admin. 2. Navigate to: https://demo.bichitrogan.com/?_route=customers/edit/{id} 3. Set: - Full Name =

```
<script>alert(1)</script>
```

- Home Address =

  ```
  <script>alert(1)</script>
  ```

4. Save changes.
5. Visit: https://demo.bichitrogan.com/?_route=customers/list
6. The payload executes in the browser.

Impact

- Session hijacking
- Credential theft
- Unauthorized actions
- Privilege escalation if admin views payload
- Application defacement

Attack Scenario

1. Attacker injects malicious payload into profile fields.
2. Payload is stored in database.
3. Admin or users view affected page.
4. Script executes in browser.
5. Attacker gains control of session or performs actions.

CVSS (Estimated)

AV:N / AC:L / PR:L / UI:R / S:C / C:H / I:H / A:L

Severity: High

Remediation

- Use htmlspecialchars(): htmlspecialchars($input, ENT_QUOTES, 'UTF-8');
- Validate input strictly.
- Implement CSP headers.
- Avoid rendering raw user input.

References

- CWE-79: https://cwe.mitre.org/data/definitions/79.html

4m3rr0r added **Analysis** 3 weeks ago

4m3rr0r added **CVE** and removed **Analysis** 5 hours ago

4m3rr0r changed the title ~~Stored Cross-Site Scripting (XSS) in Customers page (BichitroGan ISP Billing System)~~ CVE-2026-6622 5 hours ago

4m3rr0r closed this as completed 5 hours ago

Metadata

Assignees

No one assigned

Labels

CVE

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants