PEN-TEST PROVEN ASSURANCE

Date: 28-05-2026

Reviewed by: VATINS SYSTEMS PVT-LTD.

Address: Vatins Systems Private Limited, Myscape Rd, Financial District, Nanakramguda, Hyderabad, Telangana 500032

Initial Assessment Date: 27-10-2025
Final Assessment Date: 11-11-2025
Date of Revalidation: 12-02-2026

TO WHOMSOEVER IT MAY CONCERN

Company Name: Fraxion

WEB Application: Centreviews

Purpose of the WEB Application: Fraxion Centreviews is a web-based application used for centralized spend management, reporting, and workflow monitoring. It enables users to manage procurement activities, monitor transactions, and access analytical insights through role-based access controls.

Fraxion has performed remediation activities for the identified findings, and a revalidation assessment was conducted accordingly. Our analysis initially identified a total of 19 vulnerabilities. As of the latest assessment conducted on 12-02-2026, all 2 Critical, 4 High, 1 Medium, 3 Low, and 1 Informational severity vulnerabilities have been successfully addressed and verified. The remaining Medium and Low severity observations are part of the Fraxion's ongoing SDLC and remediation roadmap and will be addressed progressively as part of their regular security improvement process.

Note:

The following 7 Medium and 1 Low severity observations are not yet patched and have been acknowledged under the client's ongoing remediation and SDLC process. All Critical and High severity vulnerabilities have been successfully addressed and verified during revalidation. The remaining observations have been marked as accepted risk.

Name: Sunny NV
CEO, Vatins Systems Pvt Ltd

Assessment Methodology:

- OWASP (2025) guidelines for carrying out Web application security assessment.
- Grey box & Black box testing technique: To better understand the application functionalities and to examine possible threats associated with the application.
- We employed a hybrid methodology encompassing both manual and automated techniques to conduct the assessments.
- OSCP, CRTP, and CEH (practical) certified specialists were part of the Penetration tests conducted.

Tools Used:

Burp Suite	Tool used for intercepting and modifying requests and responses for security testing.
WSL	Tool used to run and manage a full Linux environment within Windows for executing Linux tools and scripts during security testing.

Recommendations:

- **Enforce Secure Access Controls:** Implement strict server-side validation for all users and sensitive parameters. Restrict access to critical functionalities based on user roles and permissions.
- **Protect Sensitive Data:** Implement strict authorization checks and restrict sensitive endpoints to authenticated administrative users.
- **Regular Patch Management:** Secure session cookies and keep application frameworks, libraries, and server components updated to protect against known vulnerabilities.
- **Regular VAPT:** Perform Vulnerability Assessment and Penetration Testing (VAPT) at regular intervals to identify and mitigate security vulnerabilities.

Note:

Our testing scope is confined to the staging environment exclusively; any vulnerabilities or bugs occurring in the production environment fall outside our purview.