Multiple vulnerabilities in Teampass

Posted date 31/03/2026

Identificador: INCIBE-2026-244

Importance 5 - Critical

Affected Resources

Teampass, versions prior to 3.1.5.16.

Description

INCIBE has coordinated the publication of 2 critical vulnerabilities affecting Teampass, a password manager. The vulnerabilities were discovered by Julen Garrido Estévez (B3xal).

These vulnerabilities have been assigned the following codes, CVSS v4.0 base score, CVSS vector, and CWE vulnerability type for each vulnerability:

- CVE-2026-3106 y CVE-2026-3107: CVSS v4.0: 9.1 | CVSS:

endpoint 'redacted/index.php?page=items'. The application fails to properly sanitize and encode user-input data during the import process, allowing malicious JavaScript payloads to be persistently stored in the database. When other users view the imported passwords, the payload is automatically executed in their browsers, resulting in a stored XSS condition at the endpoint 'redacted/index.php?page=items'. Exploiting this vulnerability allows an attacker to execute arbitrary JavaScript code in the context of multiple users and the administrator, which can lead to session hijacking, credential theft, privilege abuse, and compromise of application integrity.

CVE

Identificador CVE	Severidad	Explotación	Fabricante
CVE-2026-3106	Crítica	No	TEAMPASS
CVE-2026-3107	Crítica	No	TEAMPASS

Nota: El valor de explotación de cada vulnerabilidad corresponde al momento de publicación de este aviso. Dicho valor puede haber cambiado en el transcurso del tiempo.

References list

- Página web de Teampass

Update CNA Vulnerability XSS