CVE-2025-13873

TCS-CERT

Abstract Advisory Information

The product is prone to stored Cross-Site Script attacks allowing to execute arbitrary JavaScript code, into the browsing context, of any visitor of the survey.

Author: Dominique Righetto

Version affected

Name: ObjectPlanet - Opinio

Versions: 7.26 rev12562

Common Vulnerability Scoring System

Base Score: 4.8

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Patches

7.27

References

- https://www.objectplanet.com/opinio/changelog.html
- https://www.cve.org/CVERecord?id=CVE-2025-13873

Vulnerability Disclosure Timeline

- 01/12/2024: Vulnerability discovery
- 10/12/2025: Vulnerability Report to TCS-CERT
- 19/12/2024: Vulnerability Report to Vendor through email : opinio@support.objectplanet.com
- 24/12/2024: Feedback asked to vendor, check if the vendor received the PoC in an encrypted archive
- 10/01/2025: New follow-up email was send to the vendor
- 13/01/2025: Vendor confirmed the reception of the PoC, vendor asked to wait 90-day period before publishing (responsible disclosure), and will try to fix the vulnerability
- 14/10/2025: Answer to vendor to acknowledge 90 days period #8753, #8741
- 10/03/2025: Vendor will release the fix by the end of this month
- 23/04/2025: An email was sent to check where they stand on the release and fixes for the three reported issues
- 21/06/2025: A feedback was requested from vendor regarding their progress
- 30/06/2025: A feedback was requested from vendor regarding their progress
- 31/07/2025: The vendor released the newer fixed version which is the Opinio Version 7.27
- 03/12/2025: CVE ID: CVE-2025-13873