



CVE-2025-15479

Cyber Solutions / Security Advisory / CVE-2025-15479

Abstract Advisory Information

A stored cross-site scripting (XSS) vulnerability was identified in the survey creation and management features of NGSurvey Enterprise Edition (version 3.6.4), which could allow authenticated users to inject malicious content affecting other users.

Author: Thomas CLAIR

Version affected

Name: Data Illusion Zumbrunn - NGSurvey

Versions: 0 to 3.6.16

Common Vulnerability Scoring System

Base Score: 5.1

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

Patches

3.6.17

References

- <https://docs.ngsurvey.com/installation-setup/change-log#id-3.6.17-2025-05-28>
- <https://www.cve.org/CVERecord?id=CVE-2025-15479>

Vulnerability Disclosure Timeline

- 22/05/2025 – Vulnerability discovered
- 22/05/2025 – Report submitted to TCS-CERT
- 27/05/2025 – Vulnerability reported to vendor support@dataillusion.com)
- 27/05/2025 – Vendor acknowledged the report and confirmed fixes in v3.6.17
- 08/01/2025 - CVE ID assigned CVE-2025-15479

Would you like a customized presentation?

If you'd like to find out more, contact us now to arrange a personal meeting with our teams.

[Contact us](#)



[Solutions](#)

[Sectors](#)

[CyberInsights](#)

[About us](#)

[Career](#)

[contact](#)

[Thales Alert System](#)

[Legal](#)

[Privacy Policy](#)

[Cookies policy](#)

[Sitemap](#)

Thales is a global technology leader with more than 81,000 employees on five continents. The Group is investing in digital and “deep tech” innovations – Big Data, artificial intelligence, connectivity, cybersecurity and quantum technology – to build a future we can all trust.

In the markets of defence and security, aerospace and space, digital identity and cybersecurity, Thales provides solutions, services and products to help its customers - companies, organisations and governments - to carry out their critical missions.

All rights reserved © Thales 2024