



XSS in default error page

IR Number

FG-IR-25-736

Published Date

Nov 18, 2025

Component

GUI

Severity

⚠ Medium

CVSSv3 Score

4.2

Impact

Execute unauthorized code or commands

CVE ID

CVE-2025-58412

Download

📄 CVRF

📄 CSAF

Summary

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).

Accept

Version	Affected	Solution
FortiADC 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiADC 7.4	7.4 all versions	Migrate to a fixed release
FortiADC 7.2	7.2 all versions	Migrate to a fixed release
FortiADC 7.1	Not affected	Not Applicable
FortiADC 7.0	Not affected	Not Applicable
FortiADC 6.2	Not affected	Not Applicable

Workarounds:

Do not use "waf_deny.html" error page or customise it to either remove the "error-info" class or to change it into a standard hardcoded message.

Acknowledgement

Fortinet is pleased to thank ShenkerGroup and Italian ACN (National Authority Cybersecurity) for reporting this vulnerability under responsible disclosure.

Timeline

2025-11-18: Initial publication

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).

[Contact Us](#) | [Legal](#) | [Privacy](#) | [Partners](#) | [Feedback](#)



Copyright © 2026 Fortinet, Inc. All Rights Reserved.

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).