**INTELLIGENCE**

Have you found a vulnerability in a WordPress plugin or theme? Report vulnerabilities in WordPress plugins and themes through our **bug bounty program** and earn a bounty on all in-scope submissions, while we handle the responsible disclosure process on your behalf.

As a reminder, the Wordfence Intelligence Vulnerability Database API is completely free to query and utilize, both personally and commercially, and contains all the same vulnerability data as the user interface. Please review the API documentation and Webhook documentation for more information on how to query the vulnerability API endpoints and configure webhooks utilizing all the same data present in the Wordfence Intelligence user interface.

Smart Framework <= Multiple Plugins - Missing Authorization to Authenticated (Subscriber+) Stored Cross-Site Scripting

6.4
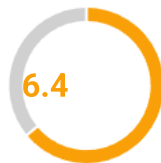
Missing Authorization
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVE	CVE-2024-13419
CVSS	6.4 (Medium)
Publicly Published	May 1, 2025
Last Updated	May 2, 2025
Researcher	Lucio Sá

Description

Multiple plugins and/or themes for WordPress using Smart Framework are vulnerable to Stored Cross-Site Scripting due to a missing capability check on the saveOptions() and importThemeOptions() functions in various versions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings which includes custom JavaScript that is enabled site-wide. This issue was escalated to Envato over two months from the date of this disclosure and the issue is still vulnerable.

References

- themeforest.net

Share

Facebook   Twitter   LinkedIn   Email

4 affected software packages

April Framework

Software Type	Plugin
Software Slug	april-framework
Patched?	✖ No
Remediation	No known patch available. Please review the vulnerability's details in depth and employ mitigations based on your

Auteur Framework

Software Type	Plugin
Software Slug	g5plus-auteur
Patched?	✖ No
Remediation	No known patch available. Please review the vulnerability's details in depth and employ mitigations based on your

Affected Version	<= 5.1 ⓘ

Software Type	Plugin
Software Slug	benaa-framework
Patched?	✖ No
Remediation	No known patch available. Please review the vulnerability's details in depth and employ mitigations based on your organization's risk tolerance. It may be best to uninstall the affected software and find a replacement.
Affected Version	<= 4.0.0 ⓘ

Affected Version	<= 7.1 ⓘ

Software Type	Plugin
Software Slug	beyot-framework
Patched?	✖ No
Remediation	No known patch available. Please review the vulnerability's details in depth and employ mitigations based on your organization's risk tolerance. It may be best to uninstall the affected software and find a replacement.
Affected Version	<= 6.0.6 ⓘ

Did you know Wordfence Intelligence provides free personal and commercial API access to our comprehensive WordPress vulnerability database, along with a free webhook integration to stay on top of the latest vulnerabilities added and updated in the database? Get started today!

LEARN MORE

Want to get notified of the latest vulnerabilities that may affect your WordPress site?
Install Wordfence on your site today to get notified immediately if your site is affected by a vulnerability that has been added to our database.

GET WORDFENCE

The Wordfence Intelligence WordPress vulnerability database is completely free to access and query via API. Please review the documentation on how to access and consume the vulnerability data via API.

DOCUMENTATION

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service

Privacy Policy and Notice at Collection

Products

Wordfence Free
Wordfence Premium
Wordfence Care

Support

Documentation
Learning Center
Free Support

News

Blog
In The News
Vulnerability Advisories

About

About Wordfence
Affiliate Program
Careers

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

☐ By checking this box I agree to the terms of service and privacy policy.*

SIGN UP

ISO 27001 CERTIFICATION

INTERCERT