



# Epsilon Framework Themes (Various Versions) - Unauthenticated Plugin Activation/Deactivation

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-36721
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-07 02:15:12 UTC
<b>Updated</b>	2026-04-08 19:17:34 UTC
<b>Description</b>	The Brilliance <= 1.2.7, Activello <= 1.4.0, and Newspaper X <= 1.3.1 themes for WordPress are vulnerable to Plugin Activation/Deactivation without authentication.

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

**EPSS:** 0.001780000 probability, percentile 0.393760000 (date 2026-04-09)

**Problem Types:** CWE-284 | CWE-862 | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	security@wordfence.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Colorlib	Activello	All	All	All	All
Application	Colorlib	Bonkers	All	All	All	All
Application	Colorlib	Illdy	All	All	All	All
Application	Colorlib	Newspaper X	All	All	All	All
Application	Colorlib	Pixova Lite	All	All	All	All
Application	Colorlib	Shapely	All	All	All	All
Application	Cpothemes	Affluent	All	All	All	All
Application	Cpothemes	Allegiant	All	All	All	All
Application	Cpothemes	Brilliance	All	All	All	All
Application	Cpothemes	Transcend	All	All	All	All
Application	Machothemes	Antreas	All	All	All	All
Application	Machothemes	Medzone Lite	All	All	All	All
Application	Machothemes	Naturemag Lite	All	All	All	All
Application	Machothemes	Newsmag	All	All	All	All
Application	Machothemes	Regina Lite	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wpchill	Brilliance	affected 1.2.7 semver	Not specified
CNA	Silkalns	Newspaper X	affected 1.3.1 semver	Not specified
CNA	Silkalns	Activello	affected 1.4.0 semver	Not specified

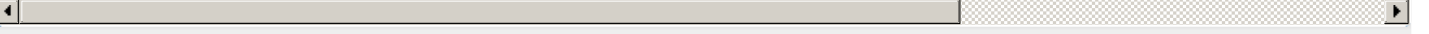
### References

Reference	Source
Unauthenticated function injection vulnerability fixed in 15 WordPress themes. – NinTechNet	af854a3a-2127-422b-91ae-364da2661108
Newspaper X – WordPress theme   WordPress.org	af854a3a-2127-422b-91ae-364da2661108
Brilliance – WordPress theme   WordPress.org	af854a3a-2127-422b-91ae-364da2661108

Epsilon Framework Themes (Various Versions) - Unauthenticated Plugin Activation/Deactivation af854a3a-2127-422b-91ae-364da2661108

CVE Program record CVE.ORG

NVD vulnerability detail NVD



Vendor Comments And Credit

Discovery Credit

**CNA:** Jerome Bruandet (en)

Additional Advisory Data

Source	Time	Event
CNA	2020-10-01T00:00:00.000Z	Disclosed

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)