WP NG Weather <= 1.0.9 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode Attributes

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-1822
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-21 04:16:54 UTC
Updated	2026-04-22 21:32:08 UTC
Description	The WP NG Weather plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ng-weather' shortco

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from security@wordfence.com

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

EPSS: 0.000370000 probability, percentile 0.110260000 (date 2026-04-22)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tonysamperi	WP NG Weather	affected 1.0.9 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/1592108b-acc0-47da-bbff-3202c...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/wp-ng-weather/tags/1.0.9/templates/app.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/wp-ng-weather/tags/1.0.9/wp-weather.php	security@wordfence.com	plugins.trac.wordpress.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Muhammad Yudha - DJ (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-20T15:18:16.000Z	Disclosed

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

CVE.report and Source URL Uptime Status status.cve.report