An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2606030221

NCSC Advisory

Actively Exploited Critical Vulnerability in Burst Statistics WordPress Analytics

CVE-2026-8181

3rd, June 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-8181

Published: 2026-05-14

Vendor: burstbv

Product: Burst Statistics – Privacy-Friendly WordPress Analytics (Google Analytics Alternative)

CVSS Score[1]: 9.8

Products Affected

Product	Version
Burst Statistics – Privacy-Friendly WordPress Analytics (Google Analytics Alternative)	3.4.0 <= 3.4.1.1

Impact

The Burst Statistics – Privacy-Friendly WordPress Analytics (Google Analytics Alternative) plugin for WordPress is vulnerable to Authentication Bypass in versions 3.4.0 to 3.4.1.1. This is due to incorrect return-value handling in the is_mainwp_authenticated() function when validating application passwords from the Authorization header.

This makes it possible for unauthenticated attackers, **with knowledge of an administrator username**, to impersonate that administrator for the duration of the request by supplying any random Basic Authentication password achieving privilege escalation.

Common Weakness Enumeration (CWE)[2]: CWE-287: Improper Authentication

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from burstbv.

If a patched version cannot be applied immediately, oranisations should disable or deactivate the Burst Statistics plugin on affected sites. Organisations should also enforce unique, non-guessable administrator usernames and remove default or predictable accounts such as admin as part of their cyber hygiene.

- https://nvd.nist.gov/vuln/detail/CVE-2026-8181
- https://www.cve.org/CVERecord?id=CVE-2026-8181
- https://www.wordfence.com/threat-intel/vulnerabilities/id/8ca830d6-3d3c-4026-85cd-8447b8a568d3?source=cve
- https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Frontend/class-mainwp-proxy.php#L336
- https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Frontend/class-mainwp-proxy.php#L336
- https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Frontend/class-mainwp-proxy.php#L328
- https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Frontend/class-mainwp-proxy.php#L328
- https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Frontend/class-mainwp-proxy.php#L314
- https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Frontend/class-mainwp-proxy.php#L314
- https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Traits/trait-admin-helper.php#L205
- https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Traits/trait-admin-helper.php#L205
- https://github.com/Burst-Statistics/burst-statistics/blob/2488d3fa54045e7e5342b0445b9f6b5eaac9ea7c/includes/Frontend/class-mainwp-proxy.php#L385