CERT-EU

Security Advisory 2024-001

Vulnerability in Wordpress Google Fonts Plugin

January 3, 2024 — v1.0

TLP:CLEAR

History:

- *03/01/2024 — v1.0 – Initial publication*

Summary

On January 2, 2024, an unauthenticated Stored Cross-Site Scripting (XSS) and directory deletion vulnerability has been discovered in the "*OMGF | GDPR/DSGVO Compliant, Faster Google Fonts. Easy.*" plugin for WordPress. This vulnerability, identified as `CVE-2023-6600` (CVSS score of 8.6)[1], may allow unauthenticated attackers to update the plugin's settings and inject malicious scripts into affected sites [2].

This vulnerability could affect sites that have the OMGF plugin installed and configured, which is estimated to be over 300,000 sites [3].

Technical Details

The OMGF plugin vulnerability occurs due to a missing capability check on the `update_settings()` function hooked via `admin_init`. This allows unauthenticated attackers to modify the plugin's settings, leading to Stored Cross-Site Scripting and directory deletion.

Affected Products

"*OMGF | GDPR/DSGVO Compliant, Faster Google Fonts. Easy.*" plugin version 5.7.9 and below.

Recommendations

To mitigate this vulnerability, users should update the vulnerable plugin to at least version 5.7.10 as it contains the necessary fixes.

Users are also advised to monitor their WordPress sites for any signs of unauthorised changes, such as injected scripts or deleted directories.

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2023-6600

[2] https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/host-webfonts-local/omgf-gdprdsgvo-compliant-faster-google-fonts-easy-579-missing-authorization-to-unauthenticated-directory-deletion-and-cross-site-scripting

[3] https://wordpress.org/plugins/host-webfonts-local/#description