MNDT-2021-0009

The DebugMetaData WordPress plugin contains a stored Cross Site Scripting (XSS) vulnerability.

Impact

High - Attacker can execute arbitrary JavaScript in the victim's browser. This allows the attacker to impersonate the user to the application and can be used as part of an attack to steal user credentials.

Exploitability

High - The attacker requires a user account on the application in order to inject a script. Once a script is injected, it is stored in the application and all users can be affected.

CVE Reference

CVE-2020-27356

Technical Details

To exploit the vulnerability, an attacker would need to intercept a login request and inject an arbitrary JavaScript payload into their user agent string. After successfully authenticating, to trigger this vulnerability a user would just have to navigate to their profile page `(hxxps://WORDPRESSBASEURL/wp-admin/profile.php)` and the victim's web browser will execute the JavaScript payload.

Resolution

The developer has elected not to fix the issue.

Discovery Credits

- Chuck Gabriele, Mandiant

Disclosure Timeline

- 26-OCT-2020 - Issue reported to Developer
- 27-Oct-2020 - Issue confirmed by Developer

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-27356
- https://github.com/ahmadawais/Debug-Meta-Data
- https://wordpress.org/plugins/debug-meta-data/