June 26, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Wordfence published security advisories to address vulnerabilities in multiple products. Included was a critical update for the following products:

- Social Warfare 4.4.6.4 to 4.4.7.1 (fixed in version 4.4.7.3)
- Blaze Widget 2.2.5 to 2.5.2 (fixed in version 2.5.4)
- Wrapper Link Element 1.0.2 to 1.0.3 (fixed in version 1.0.5)
- Contact Form 7 Multi-Step Addon 1.0.4 to 1.0.5 (fixed in version 1.0.7)
- Simply Show Hooks 1.2.1 to 1.2.2 (no fix available yet)

Technical Details

Several plugins for WordPress hosted on WordPress.org have been compromised and injected with malicious PHP scripts. A malicious threat actor compromised the source code of various plugins and injected code that exfiltrates database credentials and is used to create new, malicious, administrator users and send that data back to a server. Currently, not all plugins have been patched and we strongly recommend uninstalling the plugins for the time being and running a complete malware scan.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at VulnerabilityandRiskManagement@gov.bc.ca

References

- CVE-2024-6297
- Several WordPress.org Plugins <= Various Versions - Injected Backdoor (wordfence.com)
- Plugins on WordPress.org backdoored in supply chain attack (bleepingcomputer.com)