TLP:CLEAR

MEDIUM (Share within 24 hrs) Distribution Urgency

March 25, 2026

Cyber Security Advisory – WordPress Guidance and Best Practices

Executive Summary

Recent reports indicate that organizations operating WordPress-based websites have been impacted by security incidents stemming from misconfigurations and related weaknesses. This threat advisory provides guidance and recommended best practices to help reduce exposure and mitigate associated risks.

Content management systems remain frequent targets for attackers who exploit outdated components, weak authentication, misconfigurations, insufficient monitoring, and inadequate vendor governance. In some cases, malicious code may be introduced to alter site behaviour such as presenting alternate versions of pages or delivering malware. Implementing best practices reduces exposure and strengthens overall cyber resilience.

How does this affect my organization?

- Malicious code may be inserted into a website to present alternate or hidden versions of content based on referral source or user behaviour.
- Attackers may attempt watering hole attacks by modifying trusted websites to deliver malware through drive by downloads.
- A website exposing unnecessary ports or services increases the likelihood of automated scanning and exploitation.
- Outdated plugin themes or WordPress core components greatly expands the attack surface.

- Weak authentication and lack of Multi Factor Authentication (MFA) significantly increase the probability of administrative credential compromise.
- Insufficient logging reduces visibility into unauthorized modifications or malicious activity.
- Vendor managed hosting environments may not apply proper hardening patching or monitoring controls.

What should I do?

As soon as possible:

- **Forward this advisory** to your cyber security, network operations, and IT teams.
- Request they **review, assess, and implement** appropriate risk-mitigation measures, including:
    - Enforce MFA for all administrative access.
    - Patch WordPress core plugins and themes and remove unused or unsupported components.
    - Ensure admin portals are behind VPN or firewall restrictions and not exposed directly to the internet.
    - Disable file editing functions in wp admin and apply strict file permissions.
    - Enable detailed logging for authentication events, file and configuration changes and plugin activity.
    - Review all internet exposed systems and close unnecessary ports or services.
    - Confirm vendor responsibilities for patching, monitoring and incident response and ensure these are documented.
    - Maintain secure tested offline backups to restore clean versions of the website if malicious code is detected.

If further guidance or sector-specific recommendations are required, we can support the follow-up.

Technical Details

Threat Actors & TTPs:

- Malicious code may selectively present alternate content to specific users allowing attackers to hide harmful activity from administrators.
- Watering hole techniques may involve injecting scripts intended to distribute malware to site visitors through drive by downloads.
- Attackers routinely scan for outdated or vulnerable plugin themes or misconfigurations and exploit them to gain initial access.
- Injected malicious files within website directories can be used to maintain persistence or alter site behaviour.
- Compromised administrative credentials enable modification of templates script insertion or data capture capabilities.
- Sites with excessively exposed ports or services provide attackers with more opportunities for reconnaissance and exploitation.

More Information:

- Hardening WordPress
- WordPress Security Hardening 2026: The Complete Guide From Server to Application
- How to improve WordPress security
- Securing WordPress

Recommended Action

Additional Recommendations:

- Enable MFA including on content management services, where possible.
- Apply security patches promptly across all systems.
- Restrict outbound network connections to authorized business destinations only.
- Review and update your cyber incident response plan.
- Verify that recent backups are available and functioning.
- Ensure endpoint protection and anti-malware software are up to date.
- Educate staff to recognize phishing attempts and suspicious messages.

For Further Information

The Cyber Security Centre of Excellence has a portal, Cyber Security Ontario, that provides IT and security professionals and change management leaders in the Ontario broader public sector with foundational learning on cyber security. The Cyber Security Ontario Portal is administered by the Cyber Security Centre of Excellence within the Cyber Security Division of the Ontario Ministry of Public and Business Service Delivery and Procurement.

To learn how the Cyber Security Centre of Excellence strengthens cyber security in the broader public sector, visit Cyber Security Centre of Excellence.

No Warranty

This Cyber Security Advisory may contain third party content and links. The Cyber Security Centre of Excellence does not control or maintain third party links and makes no representation or warranty that the link: (a) will still work when you click on it; or (b) will deliver service or content that is useful, appropriate, virus-free or reliable. It is your responsibility to determine whether to access a link or agree to receive or rely on any service or content that is made available to you.

The Cyber Security Centre of Excellence is providing information about a known threat for potential use at the sole discretion of recipients to protect against cyber threats. This notification is provided to help broader public sector organizations enable cyber preparedness and resilience.

Definitions

Cyber Security Threats or Incidents are events that may present risk to the security (i.e. confidentiality, availability or integrity) of an organization's information assets, systems and networks.

- Cyber Security **Threat** Advice is issued when **no active exploits** are observed. The purpose of threat advice is to enable organizations to prepare for and mitigate cyber threats.
- Cyber Security **Incident** Advice is issued when an **active exploit** is observed. This information is time sensitive. The purpose of incident advice is to inform organizations of an ongoing cyber incident so the organization may prepare for timely response and remediation.

Cyber Security Centre of Excellence uses the traffic light protocol (TLP) for the sharing of information with parties external to the government of Ontario with public program information with TLP:CLEAR; and non-public program information with TLP:GREEN.