Australian Government
Australian Signals Directorate

Securing Content Management Systems

First published: July 2015
Last updated: October 2021

Introduction

The security of external-facing infrastructure is critical for organisations when considering the security of their network as a whole. Even if external-facing infrastructure does not host sensitive information, there is still a significant risk to the reputation of organisations if external-facing infrastructure is tampered with.

Vulnerabilities within content management systems (CMS) installed on web servers of organisations are often exploited by malicious actors. Once a CMS has been compromised, the web server can be used as infrastructure to facilitate targeted intrusion attempts.

This publication outlines strategies for identifying and minimising the potential risk to web servers using CMS. The intended audience is individuals responsible for developing and securing websites or web applications using CMS.

Risks to content management systems

Malicious actors can use automated tools to scan the internet for vulnerabilities. If a vulnerability is found, malicious actors can attempt to exploit it to gain access to a web server. Typically these compromises are opportunistic and the result of the poor security posture of the victim rather than a targeted cyber intrusion.

Once a CMS has been compromised, malicious actors can exploit their access to:

- obtain access to authenticated and privileged areas of a web application
- upload malware to the web server to facilitate remote access, for example, web shells or remote administration tools (RATs)
- inject malicious content into legitimate webpages.

Although a web server may only host publicly releasable information, the compromise of an organisation's web server is significant as malicious actors can exploit the trust of its users. Further, malicious actors can use a compromised web server as part of a 'watering hole' attack or as command and control infrastructure to facilitate other intrusions, for example, compromising an organisation with malware that is configured to receive commands from a compromised web server.

Minimising risks and improving CMS security

The most common causes of CMS compromises are due to security oversights. Some of the most effective mitigations are listed below.

Mainstream host

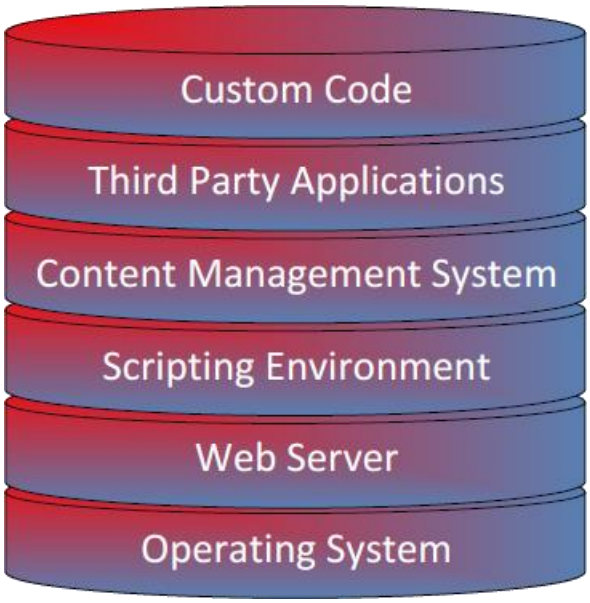
As an alternative to hosting and maintaining a CMS on your own infrastructure, consider using a managed CMS hosting service. Managed CMS hosting services maintain web infrastructure and content management applications offering support and facilitating timely patching.

Government customers can use GovCMS, which is a hosting service for Drupal-based websites.

Patch management

A common cause of a cyber intrusion is running an out-dated web server and CMS. This makes exploitation of a CMS trivial in some instances. This risk can be minimised by having an established process to test and deploy patches for the CMS, as well as patching the host operating system and third party applications, including themes, frameworks and libraries used by the CMS.

A CMS runs on a package of software known as a web stack. Additionally, organisations may employ third-party applications or custom site-specific code. All of these components (as shown below) need to be patched, as one vulnerable component could compromise the security of the other layers.



Vulnerability assessment of CMS installations

Controls that aid in assessing CMS installations for vulnerabilities include:

- using tools to scan CMS installations for vulnerabilities, for example, CMS-specific tools such as WPScan for WordPress and the Security Review module for Drupal
- conducting vulnerability assessments of custom code or modules that are used for CMS deployment.

Account management

Poor management of legitimate access can lead to the compromise of a CMS. This risk can be minimised by:

- changing default usernames and passwords, including for all related services
- using strong passphrases
- ensuring passphrases are stored by the CMS as salted hashes rather than cleartext
- restricting access to the administrator interface for the CMS from approved or internal IP addresses.

Hardening CMS installations

Controls that aid in hardening CMS installations include:

- using trusted and supported third-party plugins for the CMS
- disabling unnecessary functionality and plugins
- disabling or removing detailed debug or error messages in CMS webpages; webpages that may disclose sensitive debug information, for example phpinfo() pages, should also be removed
- removing version information that may be displayed by default on CMS webpages, for example, in the page footer or in the meta tags on each webpage; note, it is still possible to fingerprint the type and version of a CMS using automated tools
- following vendor advice on best practices for securing CMS installations.

Monitoring CMS installations

Controls that aid in the detection of unauthorised modification of content hosted on the CMS include:

- using change management to manage deployment of new versions of webpage content
- using source control to manage development of custom code
- using file integrity monitoring to manage and detect unauthorised changes to webpages.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Vendor advice on best practices for securing CMS installations is available for:

- Drupal
- WordPress
- Joomla!
- Open Web Application Security Project.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).