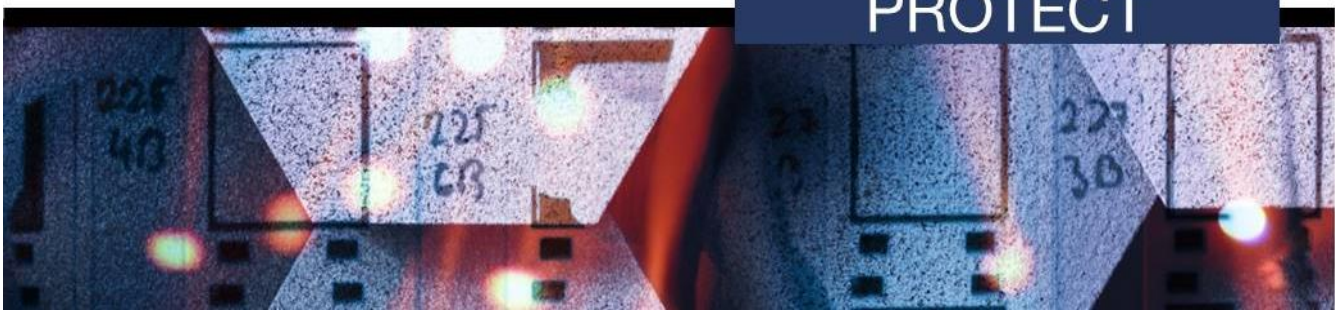

JULY 2015

Securing Content Management Systems

Introduction

1. 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.
2. Security vulnerabilities within content management systems (CMS) installed on web servers of organisations are often exploited by adversaries. Once a CMS has been compromised, the web server can be used as infrastructure to facilitate targeted intrusion attempts.

Intended audience

3. This document 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

4. An adversary can use automated tools to scan the Internet for security vulnerabilities. If a security vulnerability is found, the adversary 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.
5. Once a CMS has been compromised, an adversary can exploit their access to:
   a. obtain access to authenticated and privileged areas of a web application
   b. upload malware to the web server to facilitate remote access, for example, web shells[1] or remote administration tools (RATs)
   c. inject malicious content into legitimate webpages.
6. Although a web server may only host publicly releasable information, the compromise of an organisation's web server is significant as an adversary can exploit the trust of its users. Further, an adversary can use a compromised web server as part of a 'watering hole' attack or as

[1] https://blogs.akamai.com/2013/10/web-shells-backdoor-trojans-and-rats.html

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

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

Mainstream host

8. 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.

9. Government customers can use govCMS[2], which is a hosting service for Drupal-based websites.

10. For data that is not considered publicly releasable, use an outsourced service that has been assessed, certified and accredited against the *Australian Government Information Security Manual* (ISM). For more information, refer to the Australian Cyber Security Centre's (ACSC's) *Certified Cloud Services List*[3].

Patch management

11. 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:

    a. having an established process to test and deploy patches for the CMS

    b. patching the host operating system and third party applications, including themes, frameworks and libraries used by the CMS.

12. 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 in Figure 1) need to be patched, as one vulnerable component could compromise the security of the other layers.

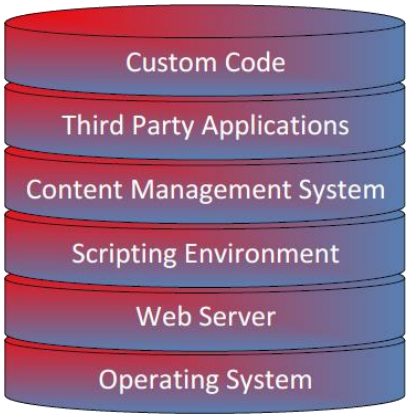

Figure 1: Components of a typical web stack

[2] https://www.govcms.gov.au

[3] https://www.acsc.gov.au

Vulnerability assessment of CMS installations

13. Security controls that aid in assessing CMS installations for security vulnerabilities include:
    a. using tools to scan CMS installations for security vulnerabilities, for example, CMS-specific tools such as WPScan for WordPress and the Security Review module for Drupal
    b. conducting vulnerability assessments of custom code or modules that are used for CMS deployment.

Account management

14. Poor management of legitimate access can lead to the compromise of a CMS. This risk can be minimised by:
    a. changing default usernames and passwords, including for all related services
    b. using strong passphrases
    c. ensuring passphrases are stored by the CMS as salted hashes rather than cleartext
    d. restricting access to the administrator interface for the CMS from approved or internal IP addresses.

Hardening CMS installations

15. Security controls that aid in hardening CMS installations include:
    a. using trusted and supported third-party plugins for the CMS
    b. disabling unnecessary functionality and plugins
    c. 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
    d. 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 such as BlindElephant[4]
    e. following vendor advice on best practices for securing CMS installations.

Monitoring CMS installations

16. Security controls that aid in the detection of unauthorised modification of content hosted on the CMS include:
    a. using change management to manage deployment of new versions of webpage content
    b. using source control to manage development of custom code
    c. using file integrity monitoring to manage and detect unauthorised changes to webpages.
17. Monitoring services that track compromised websites, such as https://www.zone-h.org and http://www.xssed.com, can be used to check if a website has been defaced. These websites are limited though in that they rely on user reporting, and hence generally only list public website defacements. It is highly unlikely that in the event that a CMS is compromised, and used as command and control infrastructure, it will be listed on these types of websites.

[4] https://community.qualys.com/community/blindelephant

Further information

18. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

19. Vendor advice on best practices for securing CMS installations can be found at:

    a. Drupal: https://www.drupal.org/docs/develop/security

    b. WordPress: https://codex.wordpress.org/Hardening_WordPress

    c. Joomla!: https://docs.joomla.org/Security_Checklist

    d. Open Web Application Security Project: https://www.owasp.org.

Contact details

20. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).