Configuration

Outdated CMS Version

The use of an outdated version of a content management system (CMS) can lead to various security issues. A list of known security vulnerabilities sorted by version number can be found in the publicly accessible CVE Details database[1]. In many cases the only countermeasure is to update to the latest version.

Solution

The best protection against security vulnerabilities due to outdated versions are regular updates. Always use the current version and check periodically for new updates. This also applies for plugins, themes and other third party products used in combination with your CMS.

- [1] http://www.cvedetails.com/

Vulnerable CMS Version

Your Content Management System (CMS) has known security vulnerabilities which can be found in the publicly accessible CVE Details database[1]. Depending on the severity of the vulnerability this may cause security incidents like confidential information disclosure, bypassing access control mechanisms,attacks against users as well as a take-over of your systems by an attacker.

Solution

Stay informed about known vulnerabilities of your CMS and follow instructions of the vendor to fix security issues. Furthermore, always use the latest version and check periodically for new updates. This also applies for plugins, themes and other third party products used in combination with your CMS.

- [1] http://www.cvedetails.com/

Downloadable Source Code

Source code on your web site can be accessed and downloaded. While this is not considered as a security vulnerability per se, this may provide valuable information to an attacker for a successful attack, such as programming language specific security holes, version numbers located in the source code, programming errors and bugs that lead to possible attacks, etc.

Solution

Make sure your source code is securely stored and it can not be accessed by unauthorized persons.

Revision #1
Created 2021-08-02 06:23:55 UTC by Patrick Wall
Updated 2021-08-02 06:42:35 UTC by Patrick Wall