Apache Module: ModSecurity

- Overview
- Usage
- Requirements
- Compatibility
  - Rule compatibility
- How to install or uninstall mod_security2
  - In the interface
  - On the command line
- Configuration
  - Configuration details
    - cPanel & WHM version 56 or earlier
    - cPanel & WHM version 58 or later
- ModSecurity utilities
  - ModSecurity SDBM
  - ModSecurity Audit Log Collector (mlogc)
- Additional documentation

Overview

The `mod_security2` Apache module provides the ModSecurity™ web application firewall for Apache.

Warnings:

- This document **only** applies to systems that run EasyApache 4.
- If your ruleset contains rule ID conflicts or syntactical errors, ModSecurity will fail and Apache will **not** start. For more information about how EasyApache handles issues with your ModSecurity rules, read the Compatibility section.

Usage

Use the `mod_security2` Apache module to install the ModSecurity web application firewall. You can configure this module to protect your Apache web applications from various attacks. The ModSecurity web application firewall also provides additional tools to monitor your Apache web server.

Requirements

This module possesses no additional requirements.

Compatibility

Rule compatibility

Major versions of the `mod_security2` Apache module use different syntaxes for ModSecurity rules.

An existing bug with ModSecurity2, the `mod_ruid2`, and `mod_mpm_itk` Apache modules causes some tracking functionality to **not** work properly with per-user MPMs. If your system uses either the `mod_ruid2` or the `mod_mpm_itk` Apache modules and also uses Persistant Storage with the initcol, setuid, or setsid directives in the ModSecurity rules, Apache will **fail** to track that rule. Apache will also log errors to its `error_log` file. For example, the IP Reputation rule in the OWASP core ruleset may give this error. cPanel, Inc. **cannot** fix this bug, as this is a ModSecurity2 issue. For more information, read the ModSecurity bug report.

Warnings:

- No conversion utility exists to rewrite rules between versions.
- Minor versions of ModSecurity may also include syntactical changes that are incompatible with older rulesets.

How to install or uninstall mod_security2

Important:

- After you install the `mod_security2` Apache module, you **must** configure the application in WHM's *ModSecurity™ Configuration* interface (*WHM >> Home >> Security Center >> ModSecurity™ Configuration*).
- To ensure the persistency of your selections, we **strongly** recommend that you use a profile to install and uninstall the `mod_security2` Apache module. For more information about profiles in EasyApache 4, read our EasyApache 4 - Create a Profile documentation.

In the interface

The easiest way to install or uninstall the `mod_security2` Apache module is to use WHM's *EasyApache 4* interface (*WHM >> Home >> Software >> EasyApache 4*).

On the command line

To install the `mod_security2` Apache module in EasyApache 4, run the following command on the command line:

```
yum install ea-apache24-mod_security2
```

To uninstall the `mod_security2` Apache module in EasyApache 4, run the following command on the command line:

```
yum remove ea-apache24-mod_security2
```

Configuration

EasyApache 4 enables the `mod_security2` Apache module for all virtual hosts by default, **except** for the default virtual host.

You can configure your ModSecurity installation in WHM's *ModSecurity Configuration* interface (*WHM >> Home >> Security Center >> ModSecurity™ Configuration*).

Configuration details

The section for the default virtual host in your `/etc/apache2/conf/httpd.conf` file contains the following directive:

```
<IfModule mod_security2.c>
    SecRuleEngine Off
</IfModule>
```

By default, the `mod_security2` Apache module stores its log file in the `/etc/apache2/logs/modsec_audit.log` file.

Important:

- EasyApache 4 adds information to the log files as the user. This action causes the system to use more disk space.
- EasyApache 4 installs the `mod_security2` Apache module with several include files.

cPanel & WHM version 56 or earlier

- When you install the `mod_security2` Apache module, the installation places the following files into your `/etc/apache2/conf.d` direc

tory:

```
modsec2.conf
modsec2.cpanel.conf
```

When the system loads, it uses the `conf.d/*.conf` glob file to pull the files into your configuration.

- In EasyApache 4, the `/etc/apache2/conf.d/modsec2.conf` file contains the basic directives for the `mod_security2` Apache module, and the following `Include` directives :

```
Include "/etc/apache2/conf.d/modsec2.user.conf"
Include "/etc/apache2/conf.d/modsec2.cpanel.conf"
```

- The `/etc/apache2/conf.d/modsec2.user.conf` file contains the ModSecurity firewall application rules that you define.

> **Warning:**
> We **strongly** recommend that you do **not** use `Include` directives in the `modsec2.user.conf` file. When you convert to EasyApache 4, the system comments out any `Include` directives and you **must** manually verify the paths.

cPanel & WHM version 58 or later

- When you install the `mod_security2` RPM, the installation places the following files into your `/etc/apache2/conf.d/modsec/` direc tory:

```
modsec2.user.conf
modsec2.cpanel.conf
```

The installation places the following file into your `/etc/apache2/conf.d/` directory:

```
/etc/apache2/conf.d
```

When the system loads, it uses the `conf.d/*.conf` glob file to pull the files into your configuration.

- In EasyApache 4, the `/etc/apache2/conf.d/modsec2.conf` file contains the basic directives for the `mod_security2` Apache module, and the following `I nclude` directives :

```
Include "/etc/apache2/conf.d/modsec/modsec2.user.conf"
Include "/etc/apache2/conf.d/modsec/modsec2.cpanel.conf"
```

The `/etc/apache2/conf.d/modsec/modsec2.user.conf` file contains the ModSecurity firewall application rules that you define.

> **Warning:**
> We **strongly** recommend that you do **not** use `Include` directives in the `modsec2.user.conf` file. When you convert to EasyApache 4, the system comments out any `Include` directives and you **must** manually verify the paths.

ModSecurity utilities

ModSecurity SDBM

cPanel & WHM provides the ModSecurity SDBM utility to purge expired entries from the `/var/cpanel/secdatadir/users/username/ip.pag` cache file, where `username` represents the cPanel username. For more information, read our ModSecurity SDBM Utility documentation.

ModSecurity Audit Log Collector (mlogc)

cPanel & WHM includes the ModSecurity Audit Log Collector (mlogc) with the ModSecurity installation. Mlogc implements remote logging of your ModSecurity audit logs. For more information, read the mlogc documentation.

You can also install or uninstall mlogc in WHM's *EasyApache 4* interface (*WHM >> Home >> Software >> EasyApache 4*).

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- ModSecurity — This website includes ModSecurity 1.x to 2.x Migration Matrix documentation.
- The ModSecurity mailing list — The ModSecurity users' mailing list.
- ModSecurity SDBM Utility – The ModSecurity SDBM utility.

- Apache Module: ModSecurity
- Apache Module: FCGId
- Apache Module: HTTP2
- Apache Module: MPM ITK
- Apache Module: Evasive

- Tutorial - Create a ModSecurity Vendor
- Guide to Report Receiver APIs for the ModSecurity Rule Reports
- UAPI Functions - LangPHP::php_get_impacted_domains
- WHM API 1 Sections - ModSecurity
- UAPI Modules - ModSecurity