



# CVE-2022-39955

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2022-39955
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnerability@ncsc.ch
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-20 07:15:00 UTC
<b>Updated</b>	2023-11-07 03:50:00 UTC
<b>Description</b>	The OWASP ModSecurity Core Rule Set (CRS) is affected by a partial rule set bypass by submitting a specially crafted HT

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	Debian Linux	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	Fedora	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	Fedora	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	Fedora	37	All	All	All
Application	<a href="#">Owasp</a>	Owasp Modsecurity Core Rule Set	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 36 Update: mod_security-2.9.6-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.c</a>
[SECURITY] Fedora 35 Update: mod_security-2.9.6-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.c</a>
[SECURITY] Fedora 37 Update: mod_security_crs-3.3.4-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.c</a>
OWASP ModSecurity Core Rule Set: Multiple Vulnerabilities (GLSA 202305-25) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
[SECURITY] Fedora 35 Update: mod_security-2.9.6-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.c</a>
[SECURITY] Fedora 37 Update: mod_security_crs-3.3.4-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.c</a>
[SECURITY] [DLA 3293-1] modsecurity-crs security update	MLIST	<a href="#">lists.debian.org</a>
[SECURITY] Fedora 36 Update: mod_security-2.9.6-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.c</a>
CRS Version 3.3.3 and 3.2.2 (covering several CVEs) – OWASP ModSecurity Core Rule Set	CONFIRM	<a href="#">coreruleset.org</a>

## Vendor Comments And Credit

## Discovery Credit

**LEGACY:** @terjanq (Jan Gora)

## Legacy QID Mappings

[181522](#) Debian Security Update for modsecurity-crs (DLA 3293-1)[184454](#) Debian Security Update for modsecurity-crs (CVE-2022-39955)[283212](#) Fedora Security Update for mod\_security (FEDORA-2022-85a85c84b3)[283213](#) Fedora Security Update for mod\_security (FEDORA-2022-90708b46e3)[283488](#) Fedora Security Update for mod\_security (FEDORA-2022-1fd73a5285)[710728](#) Gentoo Linux OWASP ModSecurity Core Rule Set Multiple Vulnerabilities (GLSA 202305-25)© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)