



CVE-2014-0240

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

Summary

CVE	CVE-2014-0240
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-27 14:55:12 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The mod_wsgi module before 3.5 for Apache, when daemon mode is enabled, does not properly handle error codes returned by the application, which could allow a remote attacker to cause a denial of service (DoS) via a crafted request.

Risk And Classification

Primary CVSS: v2.0 6.2 from nvd@nist.gov

AV:L/AC:H/Au:N/C:C/I:C/A:C

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:H/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Modwsgi	Mod Wsgi	1.0	All	All	All

Application	Modwsgi	Mod Wsgi	1.1	All	All	All
Application	Modwsgi	Mod Wsgi	1.2	All	All	All
Application	Modwsgi	Mod Wsgi	1.3	All	All	All
Application	Modwsgi	Mod Wsgi	1.4	All	All	All
Application	Modwsgi	Mod Wsgi	1.5	All	All	All
Application	Modwsgi	Mod Wsgi	1.6	All	All	All
Application	Modwsgi	Mod Wsgi	2.0	All	All	All
Application	Modwsgi	Mod Wsgi	2.1	All	All	All
Application	Modwsgi	Mod Wsgi	2.2	All	All	All
Application	Modwsgi	Mod Wsgi	2.3	All	All	All
Application	Modwsgi	Mod Wsgi	2.4	All	All	All
Application	Modwsgi	Mod Wsgi	2.5	All	All	All
Application	Modwsgi	Mod Wsgi	2.6	All	All	All
Application	Modwsgi	Mod Wsgi	2.7	All	All	All
Application	Modwsgi	Mod Wsgi	2.8	All	All	All
Application	Modwsgi	Mod Wsgi	3.0	All	All	All
Application	Modwsgi	Mod Wsgi	3.1	All	All	All
Application	Modwsgi	Mod Wsgi	3.2	All	All	All
Application	Modwsgi	Mod Wsgi	3.3	All	All	All
Application	Modwsgi	Mod Wsgi	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Graham Dumpleton: Security release for mod_wsgi (version 3.5).	af854a3a-2127-422b-91ae-364da
Apache 'mod_wsgi' Module Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da
Security Advisory SA60094 - Red Hat update for mod_wsgi - Secunia	af854a3a-2127-422b-91ae-364da
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da
Version 3.5 — mod_wsgi 4.4.5 documentation	af854a3a-2127-422b-91ae-364da
Security Advisory SA59551 - Red Hat update for python27-mod_wsgi and python33-mod_wsgi - Secunia	af854a3a-2127-422b-91ae-364da
oss-security - Security release for mod_wsgi (version 3.5)	af854a3a-2127-422b-91ae-364da
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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