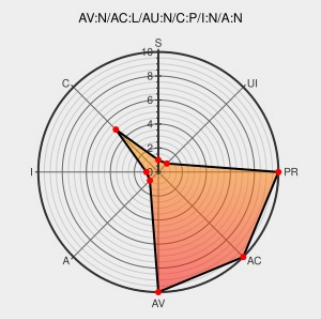
# CVE-2004-2680

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

## CVE-2004-2680

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Mod Python from Apache contain the following vulnerability:

mod_python (libapache2-mod-python) 3.1.4 and earlier does not properly handle when output filters process more than 16384 bytes, which can cause filter.read to return portions of previously freed memory.

CVE-2004-2680 has been assigned by security@ubuntu.com to track the vulnerability

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Mailing list archives | web.archive.org, text/xml, Inactive Link, Not Archived | MLIST [httpd-python-dev] 20040416 patch for filterobject.c |
| Webmail - OVH | www.vupen.com, text/html | VUPEN ADV-2007-0846 |
| Apache mod_python Output Filter Mode Information Disclosure Vulnerability | cve.report (archive), text/html | BID 22849 |
| Mailing list archives | web.archive.org, text/xml, Inactive Link, Not Archived | MLIST [httpd-python-dev] 20040416 Re: possible bug in filter.write() |
| Ubuntu update for modpython - Advisories - Secunia | web.archive.org, text/html | SECUNIA 24424 |

| | | |
|---|---|---|
| No Description Provided | issues.rpath.com<br>Inactive Link Not Archived | CONFIRM issues.rpath.com/browse/RPL-1105 |
| [Apache-SVN] Diff of /httpd/mod_python/trunk/src/filterobject.c | svn.apache.org<br>text/x-diff | CONFIRM svn.apache.org/viewvc/httpd/mod_python/trunk/src/filterobject.c?r1=102649&r2=103561&pathrev=103561 |
| USN-430-1: mod_python vulnerability \| Ubuntu | www.ubuntu.com<br>text/html | UBUNTU USN-430-1 |
| Mailing list archives | web.archive.org<br>text/xml<br>Inactive Link Not Archived | MLIST [httpd-python-dev] 20040416 possible bug in filter.write() |
| Bug #89308 “buffer leak in outputfilter” : Bugs : libapache2-mod-python package : Ubuntu | Patch<br>launchpad.net<br>text/html | CONFIRM launchpad.net/bugs/89308 |
| rPath update for mod_python - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 24418 |
| SecurityFocus | www.securityfocus.com<br>text/html | BUGTRAQ 20070307 rPSA-2007-0051-1 mod_python |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF modpython-outputfilter-info-disclosure(14751) |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Apache | Mod Python | All | All | All | All |

cpe:2.3:a:apache:mod_python:*:*:*:*:*:*:*:*:

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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**