

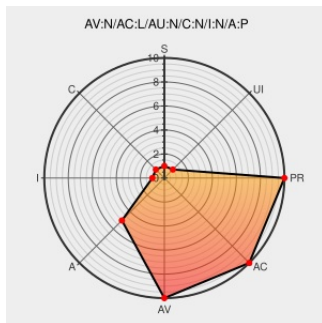


CVE-2005-1266

Published on: 06/15/2005 04:00:00 AM UTC

Last Modified on: 02/13/2023 01:15:00 AM UTC

CVE-2005-1266

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Spamassassin](#) from [Apache](#) contain the following vulnerability:

Apache SpamAssassin 3.0.1, 3.0.2, and 3.0.3 allows remote attackers to cause a denial of service (CPU consumption and slowdown) via a message with a long Content-Type header without any boundaries.

CVE-2005-1266 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Repository / Oval Repository

oval.cisecurity.org
text/html

[OVAL oval.org/mitre/oval:def:10901](https://oval.org/mitre/oval:def:10901)

Advisories - Mandriva

www.mandriva.com
text/html

[MANDRAKE MDKSA-2005:106](#)

SpamAssassin Malformed Email Header Remote Denial Of Service Vulnerability

[cve.report \(archive\)](#)
text/html

[CVE BID 13978](#)

Debian -- Security Information -- DSA-736-1 spamassassin

www.debian.org
Depreciated Link
text/html

[DEBIAN DSA-736](#)

Gentoo Linux Documentation -- SpamAssassin 3, Vipul's Razor: Denial of Service vulnerability

[Patch](#)
security.gentoo.org
text/html

[GENTOO GLSA-200506-17](#)

Mailing list archives	mail-archives.apache.org text/xml	MLIST [spamassassin-announce] 20050615 Denial of Service Vulnerability in Apache SpamAssassin 3.0.1-3.0.3
VuXML: p5-Mail-SpamAssassin -- denial of service vulnerability	Patch www.vuxml.org text/html	CONFIRM www.vuxml.org/freebsd/cc4ce06b-e01c-11d9-a8bd-000cf18bbe54.html
rhn.redhat.com Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:498
Gentoo Bug 94722 - mail-filter/spamassassin-3.*: Denial of Service (CAN-2005-1266)	Patch bugs.gentoo.org text/html	MISC bugs.gentoo.org/show_bug.cgi?id=94722

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	Spamassassin	3.0.1	All	All	All
Application	Apache	Spamassassin	3.0.2	All	All	All
Application	Apache	Spamassassin	3.0.3	All	All	All
Application	Apache	Spamassassin	3.0.1	All	All	All
Application	Apache	Spamassassin	3.0.2	All	All	All
Application	Apache	Spamassassin	3.0.3	All	All	All
cpe:2.3:a:apache:spamassassin:3.0.1:*:*:*:*:*:						
cpe:2.3:a:apache:spamassassin:3.0.2:*:*:*:*:*:						
cpe:2.3:a:apache:spamassassin:3.0.3:*:*:*:*:*:						
cpe:2.3:a:apache:spamassassin:3.0.1:*:*:*:*:*:						
cpe:2.3:a:apache:spamassassin:3.0.2:*:*:*:*:*:						
cpe:2.3:a:apache:spamassassin:3.0.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)