



CVE-2006-2447

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2006-2447
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-06 21:06:00 UTC
Updated	2018-10-18 16:40:00 UTC
Description	SpamAssassin before 3.1.3, when running with vpopmail and the paranoid (-P) switch, allows remote attackers to execute a

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Spamassassin	3.1.0	All	All	All
Application	Apache	Spamassassin	3.1.1	All	All	All
Application	Apache	Spamassassin	3.1.2	All	All	All
Application	Apache	Spamassassin	3.1.0	All	All	All
Application	Apache	Spamassassin	3.1.1	All	All	All
Application	Apache	Spamassassin	3.1.2	All	All	All

References

Reference	Source
Secunia - Advisories - Gentoo update for Spamassassin	SECUNIA
(Red Hat Issues Fix) SpamAssassin handle_user() Bug Lets Remote Users Execute Arbitrary Commands - SecurityTracker	SECTRACK
Secunia - Advisories - SpamAssassin "spamd" Shell Command Injection Vulnerability	SECUNIA
2006-0034	TRUSTIX
Nabble - ANNOUNCE: Apache SpamAssassin 3.1.3 available!	CONFIRM
Secunia - Advisories - Red Hat update for spamassassin	SECUNIA
SecurityTracker.com Archives - SpamAssassin handle_user() Bug Lets Remote Users Execute Arbitrary Commands	SECTRACK
rhn.redhat.com Red Hat Support	REDHAT

IBM X-Force Exchange	XF
SpamAssassin Vpopmail and Paranoid Switches Remote Command Execution Vulnerability	BID
Secunia - Advisories - Mandriva update for spamassassin	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Advisories - Mandriva Linux	MANDRIVA
Debian update for spamassassin - Advisories - Secunia	SECUNIA
SecurityFocus	BUGTRAQ
Gentoo Linux Documentation -- SpamAssassin: Execution of arbitrary code	GENTOO
Debian -- Security Information -- DSA-1090-1 spamassassin	DEBIAN
Trustix updates for binutils / mysql / spamassassin - Advisories - Secunia	SECUNIA
Repository / Oval Repository	OVAL
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](#)