



CVE-2008-2936

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

Summary

CVE	CVE-2008-2936
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-18 19:41:00 UTC
Updated	2023-11-07 02:02:00 UTC
Description	Postfix before 2.3.15, 2.4 before 2.4.8, 2.5 before 2.5.4, and 2.6 before 2.6-20080814, when the operating system supports

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postfix	Postfix	2.3.0	All	All	All
Application	Postfix	Postfix	2.3.1	All	All	All
Application	Postfix	Postfix	2.3.10	All	All	All
Application	Postfix	Postfix	2.3.11	All	All	All
Application	Postfix	Postfix	2.3.12	All	All	All
Application	Postfix	Postfix	2.3.13	All	All	All
Application	Postfix	Postfix	2.3.14	All	All	All
Application	Postfix	Postfix	2.3.2	All	All	All
Application	Postfix	Postfix	2.3.3	All	All	All
Application	Postfix	Postfix	2.3.4	All	All	All
Application	Postfix	Postfix	2.3.5	All	All	All
Application	Postfix	Postfix	2.3.6	All	All	All
Application	Postfix	Postfix	2.3.7	All	All	All
Application	Postfix	Postfix	2.3.8	All	All	All
Application	Postfix	Postfix	2.3.9	All	All	All
Application	Postfix	Postfix	2.4.0	All	All	All
Application	Postfix	Postfix	2.4.1	All	All	All

Application	Postfix	Postfix	2.4.2	All	All	All
Application	Postfix	Postfix	2.4.3	All	All	All
Application	Postfix	Postfix	2.4.4	All	All	All
Application	Postfix	Postfix	2.4.5	All	All	All
Application	Postfix	Postfix	2.4.6	All	All	All
Application	Postfix	Postfix	2.4.7	All	All	All
Application	Postfix	Postfix	2.5.0	All	All	All
Application	Postfix	Postfix	2.5.1	All	All	All
Application	Postfix	Postfix	2.5.2	All	All	All
Application	Postfix	Postfix	2.5.3	All	All	All
Application	Postfix	Postfix	2.6.0	All	All	All
Application	Postfix	Postfix	2.3.0	All	All	All
Application	Postfix	Postfix	2.3.1	All	All	All
Application	Postfix	Postfix	2.3.10	All	All	All
Application	Postfix	Postfix	2.3.11	All	All	All
Application	Postfix	Postfix	2.3.12	All	All	All
Application	Postfix	Postfix	2.3.13	All	All	All
Application	Postfix	Postfix	2.3.14	All	All	All
Application	Postfix	Postfix	2.3.2	All	All	All
Application	Postfix	Postfix	2.3.3	All	All	All
Application	Postfix	Postfix	2.3.4	All	All	All
Application	Postfix	Postfix	2.3.5	All	All	All
Application	Postfix	Postfix	2.3.6	All	All	All
Application	Postfix	Postfix	2.3.7	All	All	All
Application	Postfix	Postfix	2.3.8	All	All	All
Application	Postfix	Postfix	2.3.9	All	All	All
Application	Postfix	Postfix	2.4.0	All	All	All
Application	Postfix	Postfix	2.4.1	All	All	All
Application	Postfix	Postfix	2.4.2	All	All	All
Application	Postfix	Postfix	2.4.3	All	All	All
Application	Postfix	Postfix	2.4.4	All	All	All
Application	Postfix	Postfix	2.4.5	All	All	All
Application	Postfix	Postfix	2.4.6	All	All	All
Application	Postfix	Postfix	2.4.7	All	All	All
Application	Postfix	Postfix	2.5.0	All	All	All

Application	Postfix	Postfix	2.5.1	All	All	All
Application	Postfix	Postfix	2.5.2	All	All	All
Application	Postfix	Postfix	2.5.3	All	All	All
Application	Postfix	Postfix	2.6.0	All	All	All

References

Reference	Source
Support / Security / Advisories // MDVSA-2008:171 Mandriva	MANDRIVA
ftp.porcupine.org/mirrors/postfix-release/official/postfix-2.5.4.HISTORY	CONFIDENTIAL
Debian -- Security Information -- DSA-1629-2 postfix	DEBIAN
[SECURITY] Fedora 9 Update: postfix-2.5.5-1.fc9	FEDORA
[#RPL-2689] postfix privilege escalation CVE-2008-2936 CVE-2008-2937 - rPath Issue Tracking System	CONFIDENTIAL
ftp.porcupine.org/mirrors/postfix-release/official/postfix-2.4.8.HISTORY	CONFIDENTIAL
Postfix <= 2.6-20080814 (symlink) Local Privilege Escalation Exploit	EXPLOIT
SecurityFocus	BUGTRAQ
ftp.porcupine.org/mirrors/postfix-release/official/postfix-2.3.15.HISTORY	CONFIDENTIAL
Fedora update for postfix - Secunia.com	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VULNERABILITY
Gentoo update for postfix - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
SUSE update for postfix - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Gmane -- Mail To News And Back Again	MLIST
IBM X-Force Exchange	XF
CXSecurity - IDS	SREAS
Postfix Symlink Dereference Bug Lets Local Users Gain Elevated Privileges - SecurityTracker	SECURITY
[SECURITY] Fedora 8 Update: postfix-2.5.5-1.fc8	FEDORA
USN-636-1: Postfix vulnerability Ubuntu security notices	UBUNTU
Advisories:rPSA-2008-0259 - rPath Wiki	CONFIDENTIAL
Debian update for postfix - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Red Hat update for postfix - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
SecurityFocus	BUGTRAQ
[security-announce] SUSE Security Announcement: postfix (SUSE-SA:2008:04	SUSE
US-CERT Vulnerability Note VU#938323	CERT
Postfix Symlink Handling and Destination Ownership Security Issues - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Repository / Oval Repository	OVAL
Postfix: Local privilege escalation vulnerability — Gentoo Linux Documentation	GENTOO
Postfix Local Information Disclosure and Local Privilege Escalation Vulnerabilities	BID

SecurityFocus	BUGTF
Ubuntu update for postfix - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
Support	REDHA
ftp.porcupine.org/mirrors/postfix-release/experimental/postfix-2.6-20080814.HIS...	CONFI
CVE Program record	CVE.O
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](#).

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