



CVE-2008-3889

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2008-3889
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-12 16:56:00 UTC
Updated	2018-10-11 20:50:00 UTC
Description	Postfix 2.4 before 2.4.9, 2.5 before 2.5.5, and 2.6 before 2.6-20080902, when used with the Linux 2.6 kernel, leaks epoll file

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6	All	All	All
Operating System	Linux	Linux Kernel	2.6	All	All	All
Application	Postfix	Postfix	2.4	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	2.4.8	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	All	All	All
Application	Postfix	Postfix	2.4	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	2.4.8	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	All	All	All

References

Reference	Source	Link
Postfix Linux epoll File Descriptor Leak Lets Local Users Deny Service - SecurityTracker	SECTRACK	securitytrack
[SECURITY] Fedora 9 Update: postfix-2.5.5-1.fc9	FEDORA	www.redhat
Support / Security / Advisories // MDVSA-2008:190 Mandriva	MANDRIVA	www.mandr
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:018	SUSE	lists.opensu
Gentoo update for postfix - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Postfix epoll File Descriptor Leak Security Issue - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
No se encontró la página Kaizen lifestyle - Albert Sellarès Blog	MISC	www.wekk.r
Postfix: Denial of Service — Gentoo Linux Documentation	GENTOO	security.gen
Fedora update for postfix - Secunia.com	SECUNIA	secunia.com
Postfix < 2.4.9, 2.5.5, 2.6-20080902 (.forward) Local DoS Exploit	EXPLOIT-DB	www.exploit
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
USN-642-1: Postfix vulnerability Ubuntu	UBUNTU	www.ubuntu
Postfix Linux-only local denial of service	CONFIRM	www.postfix
Ubuntu update for postfix - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xf
[SECURITY] Fedora 8 Update: postfix-2.5.5-1.fc8	FEDORA	www.redhat
SecurityFocus	BUGTRAQ	www.securit
Postfix 'epoll' Linux Event Handler Local Denial of Service Vulnerability	BID	www.securit
SecurityFocus	BUGTRAQ	www.securit
SecurityFocus	CONFIRM	www.securit

SecurityHeason - Postfix Linux-only local denial of service	SHEASON	securityreas
SecurityFocus	BUGTRAQ	www.securit
wiki.rpath.com/wiki/Advisories:rPSA-2008-0311	CONFIRM	wiki.rpath.cc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2017-09-28	Joshua Bressers	Not vulnerable. This issue did not affect the versions Postfix as shipped with Red Hat Enterprise Linux 7.0-7.4.

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](#)