



CVE-2014-3956

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

Summary

CVE	CVE-2014-3956
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-04 11:19:00 UTC
Updated	2017-12-29 02:29:00 UTC
Description	The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently s

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Freebsd	Freebsd	All	-	All	All
Application	Hp	Hpx	All	All	All	All
Application	Sendmail	Sendmail	8.10	All	All	All
Application	Sendmail	Sendmail	8.10.0	All	All	All
Application	Sendmail	Sendmail	8.10.1	All	All	All
Application	Sendmail	Sendmail	8.10.2	All	All	All
Application	Sendmail	Sendmail	8.11.0	All	All	All
Application	Sendmail	Sendmail	8.11.1	All	All	All
Application	Sendmail	Sendmail	8.11.2	All	All	All
Application	Sendmail	Sendmail	8.11.3	All	All	All
Application	Sendmail	Sendmail	8.11.4	All	All	All
Application	Sendmail	Sendmail	8.11.5	All	All	All
Application	Sendmail	Sendmail	8.11.6	All	All	All
Application	Sendmail	Sendmail	8.11.7	All	All	All
Application	Sendmail	Sendmail	8.12.0	All	All	All

Application	Sendmail	Sendmail	8.12.1	All	All	All
Application	Sendmail	Sendmail	8.12.10	All	All	All
Application	Sendmail	Sendmail	8.12.11	All	All	All
Application	Sendmail	Sendmail	8.12.2	All	All	All
Application	Sendmail	Sendmail	8.12.3	All	All	All
Application	Sendmail	Sendmail	8.12.4	All	All	All
Application	Sendmail	Sendmail	8.12.5	All	All	All
Application	Sendmail	Sendmail	8.12.6	All	All	All
Application	Sendmail	Sendmail	8.12.7	All	All	All
Application	Sendmail	Sendmail	8.12.8	All	All	All
Application	Sendmail	Sendmail	8.12.9	All	All	All
Application	Sendmail	Sendmail	8.13.0	All	All	All
Application	Sendmail	Sendmail	8.13.1	All	All	All
Application	Sendmail	Sendmail	8.13.2	All	All	All
Application	Sendmail	Sendmail	8.13.3	All	All	All
Application	Sendmail	Sendmail	8.13.4	All	All	All
Application	Sendmail	Sendmail	8.13.5	All	All	All
Application	Sendmail	Sendmail	8.13.6	All	All	All
Application	Sendmail	Sendmail	8.13.7	All	All	All
Application	Sendmail	Sendmail	8.13.8	All	All	All
Application	Sendmail	Sendmail	8.14.0	All	All	All
Application	Sendmail	Sendmail	8.14.1	All	All	All
Application	Sendmail	Sendmail	8.14.2	All	All	All
Application	Sendmail	Sendmail	8.14.3	All	All	All
Application	Sendmail	Sendmail	8.14.4	All	All	All
Application	Sendmail	Sendmail	8.14.5	All	All	All
Application	Sendmail	Sendmail	8.14.6	All	All	All
Application	Sendmail	Sendmail	8.14.7	All	All	All
Application	Sendmail	Sendmail	8.6.7	All	All	All
Application	Sendmail	Sendmail	8.7.10	All	All	All
Application	Sendmail	Sendmail	8.7.6	All	All	All
Application	Sendmail	Sendmail	8.7.7	All	All	All
Application	Sendmail	Sendmail	8.7.8	All	All	All
Application	Sendmail	Sendmail	8.7.9	All	All	All
Application	Sendmail	Sendmail	8.8.8	All	All	All

Application	Sendmail	Sendmail	8.9.0	All	All	All
Application	Sendmail	Sendmail	8.9.1	All	All	All
Application	Sendmail	Sendmail	8.9.2	All	All	All
Application	Sendmail	Sendmail	8.9.3	All	All	All
Application	Sendmail	Sendmail	8.10	All	All	All
Application	Sendmail	Sendmail	8.10.0	All	All	All
Application	Sendmail	Sendmail	8.10.1	All	All	All
Application	Sendmail	Sendmail	8.10.2	All	All	All
Application	Sendmail	Sendmail	8.11.0	All	All	All
Application	Sendmail	Sendmail	8.11.1	All	All	All
Application	Sendmail	Sendmail	8.11.2	All	All	All
Application	Sendmail	Sendmail	8.11.3	All	All	All
Application	Sendmail	Sendmail	8.11.4	All	All	All
Application	Sendmail	Sendmail	8.11.5	All	All	All
Application	Sendmail	Sendmail	8.11.6	All	All	All
Application	Sendmail	Sendmail	8.11.7	All	All	All
Application	Sendmail	Sendmail	8.12.0	All	All	All
Application	Sendmail	Sendmail	8.12.1	All	All	All
Application	Sendmail	Sendmail	8.12.10	All	All	All
Application	Sendmail	Sendmail	8.12.11	All	All	All
Application	Sendmail	Sendmail	8.12.2	All	All	All
Application	Sendmail	Sendmail	8.12.3	All	All	All
Application	Sendmail	Sendmail	8.12.4	All	All	All
Application	Sendmail	Sendmail	8.12.5	All	All	All
Application	Sendmail	Sendmail	8.12.6	All	All	All
Application	Sendmail	Sendmail	8.12.7	All	All	All
Application	Sendmail	Sendmail	8.12.8	All	All	All
Application	Sendmail	Sendmail	8.12.9	All	All	All
Application	Sendmail	Sendmail	8.13.0	All	All	All
Application	Sendmail	Sendmail	8.13.1	All	All	All
Application	Sendmail	Sendmail	8.13.2	All	All	All
Application	Sendmail	Sendmail	8.13.3	All	All	All
Application	Sendmail	Sendmail	8.13.4	All	All	All
Application	Sendmail	Sendmail	8.13.5	All	All	All
Application	Sendmail	Sendmail	8.13.6	All	All	All

Application	Sendmail	Sendmail	8.13.7	All	All	All
Application	Sendmail	Sendmail	8.13.8	All	All	All
Application	Sendmail	Sendmail	8.14.0	All	All	All
Application	Sendmail	Sendmail	8.14.1	All	All	All
Application	Sendmail	Sendmail	8.14.2	All	All	All
Application	Sendmail	Sendmail	8.14.3	All	All	All
Application	Sendmail	Sendmail	8.14.4	All	All	All
Application	Sendmail	Sendmail	8.14.5	All	All	All
Application	Sendmail	Sendmail	8.14.6	All	All	All
Application	Sendmail	Sendmail	8.14.7	All	All	All
Application	Sendmail	Sendmail	8.6.7	All	All	All
Application	Sendmail	Sendmail	8.7.10	All	All	All
Application	Sendmail	Sendmail	8.7.6	All	All	All
Application	Sendmail	Sendmail	8.7.7	All	All	All
Application	Sendmail	Sendmail	8.7.8	All	All	All
Application	Sendmail	Sendmail	8.7.9	All	All	All
Application	Sendmail	Sendmail	8.8.8	All	All	All
Application	Sendmail	Sendmail	8.9.0	All	All	All
Application	Sendmail	Sendmail	8.9.1	All	All	All
Application	Sendmail	Sendmail	8.9.2	All	All	All
Application	Sendmail	Sendmail	8.9.3	All	All	All
Application	Sendmail	Sendmail	All	All	All	All

References

Reference	Source
Slackware Security Advisory - sendmail Updates ≈ Packet Storm	MISC
Sendmail File Descriptor Security Vulnerability	BID
[SECURITY] Fedora 20 Update: sendmail-8.14.8-2.fc20	FEDC
openSUSE-SU-2014:0804-1: moderate: sendmail: Close file descriptors befo	SUSE
Security Advisory SA58628 - FreeBSD update for sendmail - Secunia	SECU
Sendmail 'close-on-exec' File Descriptor Error Lets Local Users Interfere With SMTP Connections in Certain Cases - SecurityTracker	SECT
Document Display HPE Support Center	CONF
The Slackware Linux Project: Slackware Security Advisories	SLAC
Mageia Advisory: MGASA-2014-0270 - Updated sendmail packages fix CVE-2014-3956	CONF
Security Advisory SA57455 - Sendmail Close-on-Exec File Descriptors Access Bypass Security Issue - Secunia	SECU
Open Source Release 8.14.9 - Sendmail.com	CONF

Support / Security / Advisories // MDVSA-2015:128 Mandriva	MANDRIVA
FreeBSD-SA-14:11	FREEBSD
Gentoo Linux Documentation -- sendmail: Information disclosure	GENTOO
openSUSE-SU-2014:0805-1: moderate: sendmail: Close file descriptors befo	SUSE
ftp.sendmail.org/pub/sendmail/RELEASE_NOTES	CONFIDENTIAL
www.mandriva.com	MANDRIVA
CVE Program record	CVE.COM
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](#)