



CVE-2013-2125

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

Summary

CVE	CVE-2013-2125
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-27 14:55:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	OpenSMTPD before 5.3.2 does not properly handle SSL sessions, which allows remote attackers to cause a denial of servi

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Opensmtpd	All	All	All	All

References

Reference	Source	Link
OpenSMTPD - The OpenSMTPD daemon	CONFIRM	git.zx2c4.com
oss-sec: CVE Request: DoS in OpenSMTPD TLS Support	MLIST	seclists.org
IBM X-Force Exchange	XF	exchange.xforce.it
93495	OSVDB	osvdb.org
Security Advisory SA53353 - OpenSMTPD SSL Session Handling Denial of Service Vulnerability - Secunia	SECUNIA	secunia.com
oss-sec: Re: Re: CVE Request: DoS in OpenSMTPD TLS Support	MLIST	seclists.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)