



CVE-2008-1383

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

Summary

CVE	CVE-2008-1383
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-18 22:44:00 UTC
Updated	2017-08-08 01:30:00 UTC
Description	The docert function in ssl-cert.eclass, when used by src_compile or src_install on Gentoo Linux, stores the SSL key in a bir

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xfc
Gentoo 'ssl-cert' eclass Information Disclosure Vulnerability	BID	www.security
43479	OSVDB	osvdb.org
ssl-cert eclass: Certificate disclosure — Gentoo Linux Documentation	GENTOO	security.gent
Gentoo Multiple ebuidls ssl-cert eclass "docert()" Security Issue - Advisories - Secunia	SECUNIA	secunia.com
Gentoo Bug 174759 - ssl-cert.eclass docert function usage in src_install can expose SSL keys (CVE-2008-1383)	CONFIRM	bugs.gentoo.
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](#).

Free CVE JSON API [cve.report/api](#)

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