



CVE-2010-2939

Published on: 08/17/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:19:00 AM UTC

CVE-2010-2939

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openssl](#) from [Openssl](#) contain the following vulnerability:

Double free vulnerability in the `ssl3_get_key_exchange` function in the OpenSSL client (`ssl/s3_clnt.c`) in OpenSSL 1.0.0a, 0.9.8, 0.9.7, and possibly other versions, when using ECDH, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted private key with an invalid prime. NOTE: some sources refer to this as a use-after-free issue.

CVE-2010-2939 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Re: openssl-1.0.0a and glibc detected sthg ;)	www.mail-archive.com text/html	MLIST [openssl-dev] 20100808 Re: openssl-1.0.0a and glibc detected sthg ;)
Debian update for openssl - Advisories - Community	web.archive.org text/html	SECUNIA 41105
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:021	lists.opensuse.org text/html	SUSE SUSE-SR:2010:021
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-2229
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-3077

Debian -- Security Information -- DSA-2100-1 openssl	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2100
OpenSSL "ssl3_get_key_exchange()" Use-After-Free Vulnerability - Advisories - Community	Vendor Advisory web.archive.org text/html	 SECUNIA 40906
openssl-1.0.0a and glibc detected sthg ;)	www.mail-archive.com text/html	 MLIST [openssl-dev] 20100807 openssl-1.0.0a and glibc detected sthg ;)
oss-security - Re: CVE Request: openssl double free	www.openwall.com text/html	 MLIST [oss-security] 20100812 Re: CVE Request: openssl double free
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20110211 VMSA-2011-0003 Third party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX
VMware ESX Server / ESXi OpenSSL Vulnerabilities - Secunia.com	web.archive.org text/html	 SECUNIA 43312
Slackware update for openssl - Secunia.com	web.archive.org text/html	 SECUNIA 42309
VMSA-2011-0003	www.vmware.com text/html	 CONFIRM www.vmware.com/security/advisories/VMSA-2011-0003.html
'[security bulletin] HPSBMA02662 SSRT100409 rev.1 - HP System Management Homepage (SMH) for Linux and' - MARC	marc.info text/html	 HP HPSBMA02662
	security.FreeBSD.org text/plain	 FREEBSD FreeBSD-SA-10:10
Full Disclosure: openssl-1.0.0a	seclists.org text/html	 FULLDISC 20100807 openssl-1.0.0a
Re: openssl-1.0.0a and glibc detected sthg ;)	www.mail-archive.com text/html	 MLIST [openssl-dev] 20100807 Re: openssl-1.0.0a and glibc detected sthg ;)
USN-1003-1: OpenSSL vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1003-1
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2010-2038
The Slackware Linux Project: Slackware Security Advisories	slackware.com text/html	 SLACKWARE SSA:2010-326-01
SecurityTracker.com Archives - OpenSSL Key Exchange Memory Corruption Error Lets Remote Users Deny Service	securitytracker.com text/html	 SECTRAK 1024296
FreeBSD update for openssl - Secunia.com	web.archive.org text/html	 SECUNIA 42413

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All

```
cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:1.0.0a:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:1.0.0a:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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