



CVE-2003-0078

Published on: 03/03/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:45 PM UTC

CVE-2003-0078

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

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

ssl3_get_record in s3_pkt.c for OpenSSL before 0.9.7a and 0.9.6 before 0.9.6i does not perform a MAC computation if an incorrect block cipher padding is used, which causes an information leak (timing discrepancy) that may make it easier to launch cryptographic attacks that rely on distinguishing between padding and MAC verification errors, possibly leading to extraction of the original plaintext, aka the "Vaudenay timing attack."

CVE-2003-0078 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

No Description Provided

[patches.sgi.com](#)

[SGI 20030501-01-I](#)

Inactive Link Not Archived

No Description Provided

[www.osvdb.org](#)

[OSVDB 3945](#)

Inactive Link Not Archived

'GLSA: openssl (200302-10)' - MARC

[marc.info](#)
[text/html](#)

[GENTOO GLSA-200302-10](#)

[ftp.netbsd.org](#)

[NETBSD NetBSD-SA2003-001](#)

	text/plain	
	Patch Vendor Advisory www.openssl.org text/x-diff	 CONFIRM www.openssl.org/news/secadv_20030219.txt
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:062
Debian -- Security Information -- DSA-253-1 openssl	Vendor Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-253
No Description Provided	marc.info text/html	 BUGTRAQ 20030219 OpenSSL 0.9.7a and 0.9.6i released
N-051: Red Hat Updated OpenSSL Packages Fix Timing Attack	web.archive.org text/html Inactive Link Not Archived	 CIAC N-051
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:104
OpenSSL CBC Error Information Leakage Weakness	cve.report (archive) text/html	 BID 6884
Mandrakesoft Security Advisories	web.archive.org text/html Inactive Link Not Archived	 MANDRAKE MDKSA-2003:020
'[OpenPKG-SA-2003.013] OpenPKG Security Advisory (openssl)' - MARC	marc.info text/html	 BUGTRAQ 20030219 [OpenPKG-SA-2003.013] OpenPKG Security Advisory (openssl)
	www.trustix.org text/plain Inactive Link Not Archived	 TRUSTIX 2003-0005
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:082
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:205
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:063
LinuxSecurity.com: EnGarde: OpenSSL timing-based attack vulnerability	www.linuxsecurity.com text/html	 ENGARDE ESA-20030220-005
ISS X-Force Database:ssl-cbc-information-leak(11369): Multiple SSL/TLS implementation CBC ciphersuites information leak	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 XF ssl-cbc-information-leak(11369)
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLSA-2003:570

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 OIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	4.2	All	All	All
Operating System	Freebsd	Freebsd	4.3	All	All	All
Operating System	Freebsd	Freebsd	4.4	All	All	All
Operating System	Freebsd	Freebsd	4.5	All	All	All
Operating System	Freebsd	Freebsd	4.6	All	All	All
Operating System	Freebsd	Freebsd	4.7	All	All	All
Operating System	Freebsd	Freebsd	4.8	pre-release	All	All
Operating System	Freebsd	Freebsd	5.0	All	All	All
Operating System	Freebsd	Freebsd	4.2	All	All	All
Operating System	Freebsd	Freebsd	4.3	All	All	All
Operating System	Freebsd	Freebsd	4.4	All	All	All
Operating System	Freebsd	Freebsd	4.5	All	All	All
Operating System	Freebsd	Freebsd	4.6	All	All	All
Operating System	Freebsd	Freebsd	4.7	All	All	All
Operating System	Freebsd	Freebsd	4.8	pre-release	All	All
Operating System	Freebsd	Freebsd	5.0	All	All	All
Operating System	Openbsd	Openbsd	3.1	All	All	All
Operating System	Openbsd	Openbsd	3.2	All	All	All
Operating System	Openbsd	Openbsd	3.1	All	All	All
Operating System	Openbsd	Openbsd	3.2	All	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All

Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All

cpe:2.3:o:freebsd:freebsd:4.2:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.3:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.5:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.7:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.8:pre-release:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:5.0:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.2:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.3:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.5:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.7:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:4.8:pre-release:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:5.0:*:*:*:*:*:
cpe:2.3:o:openbsd:openbsd:3.1:*:*:*:*:*:
cpe:2.3:o:openbsd:openbsd:3.2:*:*:*:*:*:
cpe:2.3:o:openbsd:openbsd:3.1:*:*:*:*:*:
cpe:2.3:o:openbsd:openbsd:3.2:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.1c:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.2b:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.3:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.4:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.5:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.5a:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.6:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.6a:*:*:*:*:*:
cpe:2.3:a:openssl:openssl:0.9.6b:*:*:*:*:*:

© [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](#)