



# CVE-2003-0147

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2003-0147
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2003-03-31 05:00:00 UTC
<b>Updated</b>	2018-10-19 15:29:00 UTC
<b>Description</b>	OpenSSL does not use RSA blinding by default, which allows local and remote attackers to obtain the server's private key t

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	All	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	1.1	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	1.2	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	All	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	1.1	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	1.2	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7a	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7a	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.10	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.11	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.12	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.13	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.14	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.15	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.16	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.17	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.18	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.19	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.20	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.21	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.22	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.7	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.8	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.9	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	4.0	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	4.01	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	4.02	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	4.03	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	4.04	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.10	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.11	All	All	All
Application	<a href="#">Stunnel</a>	<a href="#">Stunnel</a>	3.12	All	All	All

Application	Stunnel	Stunnel	3.13	All	All	All
Application	Stunnel	Stunnel	3.14	All	All	All
Application	Stunnel	Stunnel	3.15	All	All	All
Application	Stunnel	Stunnel	3.16	All	All	All
Application	Stunnel	Stunnel	3.17	All	All	All
Application	Stunnel	Stunnel	3.18	All	All	All
Application	Stunnel	Stunnel	3.19	All	All	All
Application	Stunnel	Stunnel	3.20	All	All	All
Application	Stunnel	Stunnel	3.21	All	All	All
Application	Stunnel	Stunnel	3.22	All	All	All
Application	Stunnel	Stunnel	3.7	All	All	All
Application	Stunnel	Stunnel	3.8	All	All	All
Application	Stunnel	Stunnel	3.9	All	All	All
Application	Stunnel	Stunnel	4.0	All	All	All
Application	Stunnel	Stunnel	4.01	All	All	All
Application	Stunnel	Stunnel	4.02	All	All	All
Application	Stunnel	Stunnel	4.03	All	All	All
Application	Stunnel	Stunnel	4.04	All	All	All

## References

Reference	Source	Link	Tag
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
20030501-01-I	SGI	<a href="http://patches.sgi.com">patches.sgi.com</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
'GLSA: stunnel (200303-24)' - MARC	GENTOO	<a href="http://marc.info">marc.info</a>	
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
'GLSA: openssl (200303-15)' - MARC	GENTOO	<a href="http://marc.info">marc.info</a>	
CSSA-2003-014.0	CALDERA	<a href="http://ftp.sco.com">ftp.sco.com</a>	
MandrakeSecure: MandrakeSoft Security Advisory MDKSA-2003:035 : openssl	MANDRAKE	<a href="http://www.mandrakesecure.net">www.mandrakesecure.net</a>	
Gentoo Linux — Error 404 (Not Found)	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
'Vulnerability in OpenSSL' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
'[ADVISORY] Timing Attack on OpenSSL' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
SecurityFocus	IMMUNIX	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
OpenPKG Corporation: Security: Security Advisories	OPENPKG	<a href="http://www.openpkg.com">www.openpkg.com</a>	
Home - Conectiva	CONNECTIVA	<a href="http://distro.conectiva.com.br">distro.conectiva.com.br</a>	

'[OpenPKG-SA-2003.026] OpenPKG Security Advisory (openssl)' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
Neohapsis Archives - VulnWatch - #0130 - [VulnWatch] OpenSSL Private Key Disclosure	VULNWATCH	<a href="http://archives.neohapsis.com">archives.neohapsis.com</a>	Ver
Debian -- Security Information -- DSA-288-1 openssl	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
<a href="http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf">crypto.stanford.edu/~dabo/papers/ssl-timing.pdf</a>	MISC	<a href="http://crypto.stanford.edu">crypto.stanford.edu</a>	
<a href="http://www.openssl.org/news/secadv_20030317.txt">www.openssl.org/news/secadv_20030317.txt</a>	CONFIRM	<a href="http://www.openssl.org">www.openssl.org</a>	
CERT/CC Vulnerability Note VU#997481	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>	Thir
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	can

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org/cve). This site includes MITRE data granted under the following [license](http://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)