CVE-2003-0147

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openpkg	Openpkg	All	All	All	All
Application	Openpkg	Openpkg	1.1	All	All	All
Application	Openpkg	Openpkg	1.2	All	All	All
Application	Openpkg	Openpkg	All	All	All	All
Application	Openpkg	Openpkg	1.1	All	All	All
Application	Openpkg	Openpkg	1.2	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	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7a	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	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Stunnel	Stunnel	3.10	All	All	All
Application	Stunnel	Stunnel	3.11	All	All	All
Application	Stunnel	Stunnel	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
Application	Stunnel	Stunnel	3.10	All	All	All
Application	Stunnel	Stunnel	3.11	All	All	All
Application	Stunnel	Stunnel	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	www.securityfocus.com	
20030501-01-I	SGI	patches.sgi.com	
redhat.com | Red Hat Support	REDHAT	www.redhat.com	
'GLSA: stunnel (200303-24)' - MARC	GENTOO	marc.info	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
'GLSA: openssl (200303-15)' - MARC	GENTOO	marc.info	
CSSA-2003-014.0	CALDERA	ftp.sco.com	
MandrakeSecure: MandrakeSoft Security Advisory MDKSA-2003:035 : openssl	MANDRAKE	www.mandrakesecure.net	
Gentoo Linux — Error 404 (Not Found)	GENTOO	www.gentoo.org	
redhat.com | Red Hat Support	REDHAT	www.redhat.com	
'Vulnerability in OpenSSL' - MARC	BUGTRAQ	marc.info	
'[ADVISORY] Timing Attack on OpenSSL' - MARC	BUGTRAQ	marc.info	
SecurityFocus	IMMUNIX	www.securityfocus.com	
OpenPKG Corporation: Security: Security Advisories	OPENPKG	www.openpkg.com	
Home - Conectiva	CONECTIVA	distro.conectiva.com.br	

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