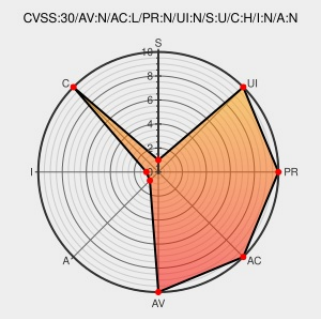
CVE-2000-1254

Published on: 05/04/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:29 PM UTC

CVE-2000-1254

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openssl from Openssl contain the following vulnerability:

crypto/rsa/rsa_gen.c in OpenSSL before 0.9.6 mishandles C bitwise-shift operations that exceed the size of an expression, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging improper RSA key generation on 64-bit HP-UX platforms.

CVE-2000-1254 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
git.openssl.org Git - openssl.git/commit	git.openssl.org text/xml	CONFIRM git.openssl.org/?p=openssl.git;a=commit;h=db82b8f9bd432a59aea8e1014694e15fc457c2bb
'64 bit problem in	marc.info	MLIST [openssl-users] 20000529 64 bit problem in BSA_generate_key

64 bit problem in RSA_generate_key in 0.9.5a' - MARC	marc.info text/html	MLIST [openssl-users] 20000620 64 bit problem in RSA_generate_key in 0.9.5a
OpenSSL *RSA_generate_key() Bit-shifting Flaw Lets Remote Users Access Data on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1035750
oss-security - broken RSA keys	www.openwall.com text/html	MLIST [oss-security] 20160504 broken RSA keys
OpenSSL CVE-2000-1254 Security Bypass Vulnerability	cve.report (archive) text/html	BID 90109
IBM Security Bulletin: Vulnerabilities in OpenSSL, OpenVPN and GNU glibc affect IBM Security Virtual Server Protection for VMware - United States	web.archive.org text/html Inactive Link Not Archived	CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21995039

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	All	All	All	All

cpe:2.3:a:openssl:openssl:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→