



CVE-2000-1254

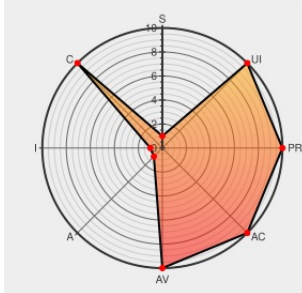
Published on: 05/04/2016 12:00:00 AM UTC

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

CVE-2000-1254

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



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 [M](#) 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

[more info](#)

[MIT IST \[openssl-users\] 20000529 64 bit problem in RSA_generate_key](#)

0.9.5a problem in
RSA_generate_key in 0.9.5a' -
MARC

marcanio

text/html

MLIST [openssl users] 20000209 0.9.5a 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

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

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](#)