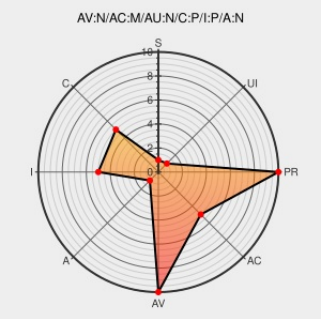
CVE-2004-2682

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2682

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



Certain versions of Matrixssl from Peersec Networks contain the following vulnerability:

PeerSec MatrixSSL before 1.1 does not implement RSA blinding, which allows context-dependent attackers to obtain the server's private key by determining factors using timing differences on (1) the number of extra reductions during Montgomery reduction, and (2) the use of different integer multiplication algorithms ("Karatsuba" and normal), a related issue to CVE-2003-0147.

CVE-2004-2682 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
MatrixSSL - RSA Blinding	www.matrixssl.org text/html	CONFIRM www.matrixssl.org/archives/000075.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Peersec Networks	Matrixssl	All	All	All	All

cpe:2.3:a:peersec_networks:matrixssl:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→