



CVE-2004-2682

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

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

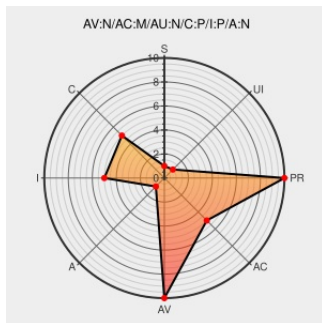
CVE-2004-2682

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 [M](#) 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](http://www.matrixssl.org/text/html)

[CONFIRM www.matrixssl.org/archives/000075.html](http://www.matrixssl.org/archives/000075.html)

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	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→		

© [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](#)