



CVE-2016-6885

Published on: 01/13/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-6885

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

Certain versions of [Matrixssl](#) from [Matrixssl](#) contain the following vulnerability:

The pstm_exptmod function in MatrixSSL before 3.8.4 allows remote attackers to cause a denial of service (invalid free and crash) via a base zero value for the modular exponentiation.

CVE-2016-6885 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	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
MatrixSSL - MatrixSSL 3.8.4	Patch Vendor Advisory www.matrixssl.org text/html	CONFIRM www.matrixssl.org/blog/releases/matrixssl_3_8_4

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	Matrixssl	Matrixssl	All	All	All	All
cpe:2.3:a:matrixssl:matrixssl:*:*:*:*:*.*						

No vendor comments have been submitted for this CVE