CVE-2016-6887

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-6887
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-13 16:59:00 UTC
Updated	2017-01-19 02:59:00 UTC
Description	The pstm_exptmod function in MatrixSSL 3.8.6 and earlier does not properly perform modular exponentiation, which might

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
MatrixSSL - MatrixSSL 3.8.4	CONFIRM	www.matrixssl.org	Patch, Vendor Advisory
Fun with Bignums: Crashing MatrixSSL and more | The Fuzzing Project	MISC	blog.fuzzing-project.org	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report