



CVE-2016-6883

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-6883
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-03 16:59:00 UTC
Updated	2017-12-15 02:29:00 UTC
Description	MatrixSSL before 3.8.3 configured with RSA Cipher Suites allows remote attackers to obtain sensitive information via a Blei

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
Page not found · GitHub · GitHub	CONFIRM	github.com	Patch, Release Notes
MatrixSSL Multiple Information Disclosure Vulnerabilities	BID	www.securityfocus.com	
oss-security - Re: CVE request: MatrixSSL lack of RSA-CRT hardening	MLIST	www.openwall.com	Mailing List
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.

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](#).

Free CVE JSON API cve.report/api

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