



CVE-2017-1000417

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-1000417
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-22 23:29:00 UTC
Updated	2018-02-13 16:18:00 UTC
Description	MatrixSSL version 3.7.2 adopts a collision-prone OID comparison logic resulting in possible spoofing of OIDs (e.g. in ExtKe

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Matrixssl	Matrixssl	3.7.2	All	All	All
Application	Matrixssl	Matrixssl	3.7.2	All	All	All

References

Reference	Source	Link
www.ieee-security.org/TC/SP2017/papers/231.pdf	MISC	www.ieee-sec
matrixssl/CHANGES.md at master · matrixssl/matrixssl · GitHub	MISC	github.com
SymCerts: Practical Symbolic Execution For Exposing Noncompliance in X.509 Certificate Validation - YouTube	MISC	www.youtube
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#)