CVE-2019-13629

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-13629
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-03 14:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	MatrixSSL 4.2.1 and earlier contains a timing side channel in ECDSA signature generation. This allows a local or a remote

Risk And Classification

Problem Types: CWE-327 | CWE-203

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
Return of the Hidden Number Problem. | IACR Transactions on Cryptographic Hardware and Embedded Systems	MISC	tches.iacr.or
minerva.crocs.fi.muni.cz	MISC	minerva.cro
eprint.iacr.org/2011/232.pdf	MISC	eprint.iacr.o
oss-security - Minerva: ECDSA key recovery from bit-length leakage	MLIST	www.openw
CVE Program record	CVE.ORG	www.cve.or
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.

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