



CVE-2019-15137

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

Summary

CVE	CVE-2019-15137
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-18 16:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	The Access Control plugin in eProsimas Fast RTPS through 1.9.0 allows fnmatch pattern matches with topic name strings (i

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eprosimas	Fast-rtps	All	All	All	All

References

Reference	Source	Link	Te
[1908.05310] Network Reconnaissance and Vulnerability Excavation of Secure DDS Systems	MISC	arxiv.org	Th
Misuse of fnmatch used by DDS Security Access Control [5346] · Issue #441 · eProsimas/Fast-DDS · GitHub	MISC	github.com	Pa
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

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