CVE-2021-34433

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-34433
State	PUBLIC
Assigner	security@eclipse.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-20 17:15:00 UTC
Updated	2021-08-26 14:02:00 UTC
Description	In Eclipse Californium version 2.0.0 to 2.6.4 and 3.0.0-M1 to 3.0.0-M3, the certificate based (x509 and RPK) DTLS handsha

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eclipse	Californium	All	All	All	All
Application	Eclipse	Californium	3.0.0	m1	All	All
Application	Eclipse	Californium	3.0.0	m2	All	All
Application	Eclipse	Californium	3.0.0	m3	All	All

References

Reference	Sourc
575281 – (CVE-2021-34433) 2.0 - 2.6 : DTLS vulnerability not verifying the server certificate, when ServerKeyExchange is not signed	CONF
CVE Program record	CVE.(
NVD vulnerability detail	NVD

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