CVE-2016-10931

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-10931
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-26 12:15:00 UTC
Updated	2023-02-27 19:19:00 UTC
Description	An issue was discovered in the openssl crate before 0.9.0 for Rust. There is an SSL/TLS man-in-the-middle vulnerability be

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl Project	Openssl	All	All	All	All
Application	Openssl Project	Openssl	All	All	All	All
Application	Rust-openssl Project	Rust-openssl	All	All	All	All

References

Reference	Source	Link
RUSTSEC-2016-0001: openssl: SSL/TLS MitM vulnerability due to insecure defaults › RustSec Advisory Database	MISC	rustsec.org
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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