RUSTSEC-2021-0076

libsecp256k1 allows overflowing signatures

Reported	July 13, 2021
Issued	July 13, 2021 (last modified: November 6, 2021)
Package	libsecp256k1 (crates.io)
Type	Vulnerability
Categories	crypto-failure
Aliases	CVE-2021-38195
Details	https://github.com/paritytech/libsecp256k1/pull/67
Patched	`>=0.5.0`

Description

libsecp256k1 accepts signatures whose R or S parameter is larger than the secp256k1 curve order, which differs from other implementations. This could lead to invalid signatures being verified.

The error is resolved in 0.5.0 by adding a `check_overflow` flag.