RUSTSEC-2021-0075

Flaw in `FieldVar::mul_by_inverse` allows unsound R1CS constraint systems

Reported	July 8, 2021
Issued	July 9, 2021 (last modified: November 6, 2021)
Package	ark-r1cs-std (crates.io)
Type	Vulnerability
Categories	crypto-failure
Keywords	#r1cs #zksnark #arkworks
Aliases	CVE-2021-38194
Details	https://github.com/arkworks-rs/r1cs-std/pull/70
Patched	`>=0.3.1`

Affected Functions	Version
`ark_r1cs_std::FieldVar::mul_by_inverse`	`<0.3.0`

Description

Versions `0.2.0` to `0.3.0` of ark-r1cs-std did not enforce any constraints in the `FieldVar::mul_by_inverse` method, allowing a malicious prover to produce an unsound proof that passes all verifier checks. This method was used primarily in scalar multiplication for `short_weierstrass::ProjectiveVar` .

This bug was fixed in commit `47ddbaa` , and was released as part of version `0.3.1` on `crates.io` .