RUSTSEC-2020-0002

History · Edit

Parsing a specially crafted message can result in a stack overflow

Reported	January 16, 2020
Issued	October 2, 2020 (last modified: October 19, 2021)
Package	prost (crates.io)
Type	Vulnerability
Categories	denial-of-service memory-corruption
Keywords	#stack-overflow
Aliases	CVE-2020-35858
Details	https://github.com/danburkert/prost/issues/267
CVSS Score	9.8 CRITICAL
CVSS Details	

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Patched	`>=0.6.1`

Description

Affected versions of this crate contained a bug in which decoding untrusted input could overflow the stack.

On architectures with stack probes (like x86), this can be used for denial of service attacks, while on architectures without stack probes (like ARM) overflowing the stack is unsound and can result in potential memory corruption (or even RCE).

The flaw was quickly corrected by @danburkert and released in version 0.6.1.