RUSTSEC-2021-0044

History · Edit

Use after free possible in `uri::Formatter` on panic

Reported	February 9, 2021	
Issued	March 26, 2021 (last modified: October 19, 2021)	
Package	rocket (crates.io)	
Type	INFO Unsound	
Categories	memory-corruption	
Keywords	#memory-safety #use-after-free	
Aliases	CVE-2021-29935	
Details	https://github.com/SergioBenitez/Rocket/issues/1534	
CVSS Score	7.3 HIGH	
CVSS Details	Attack vector	Network
	Attack complexity	Low
	Privileges required	None
	User interaction	None
	Scope	Unchanged
	Confidentiality	Low
	Integrity	Low
	Availability	Low
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	
Patched	`>=0.4.7`	

Description

Affected versions of this crate transmuted a `&str` to a `&'static str` before pushing it into a `StackVec`, this value was then popped later in the same function.

This was assumed to be safe because the reference would be valid while the method's stack was active. In between the push and the pop, however, a function `f` was called that could invoke a user provided function.

If the user provided panicked, then the assumption used by the function was no longer true and the transmute to `&'static` would create an illegal static reference to the string. This could result in a freed string being used during (such as in a `Drop` implementation) or after (e.g through `catch_unwind`) the panic unwinding.

This flaw was corrected in commit e325e2f by using a guard object to ensure that the `&'static str` was dropped inside the function.