RUSTSEC-2020-0017   History · Edit

Use after free in ArcIntern::drop

Reported	May 28, 2020
Issued	October 2, 2020 (last modified: October 19, 2021)
Package	internment (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2020-35874
Details	https://github.com/droundy/internment/issues/11
CVSS Score	8.1 HIGH

CVSS Details

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

CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Patched	`>=0.4.0`
Unaffected	`<0.3.12`

Affected Functions	Version
`internment::ArcIntern::drop`	`>=0.3.12`

Description

`ArcIntern::drop` has a race condition where it can release memory which is about to get another user. The new user will get a reference to freed memory.

This was fixed by serializing access to an interned object while it is being deallocated.

Versions prior to 0.3.12 used stronger locking which avoided the problem.