



CVE-2022-36086

Published on: Not Yet Published

Last Modified on: 07/21/2023 07:23:00 PM UTC

CVE-2022-36086 - advisory for GHSA-xg8p-34w2-j49j

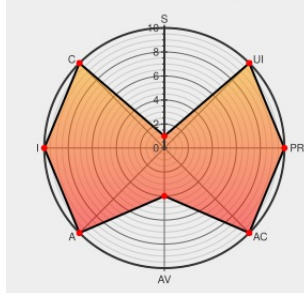
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Linked-list-allocator](#) from [Rust-osdev](#) contain the following vulnerability:

linked_list_allocator is an allocator usable for no_std systems. Prior to version 0.10.2, the heap initialization methods were missing a minimum size check for the given heap size argument. This could lead to out-of-bound writes when a heap was initialized with a size smaller than `3 * size_of::usize` because of metadata write operations. This

vulnerability impacts all the initialization functions on the `Heap` and `LockedHeap` types, including `Heap::new`, `Heap::init`, `Heap::init_from_slice`, and `LockedHeap::new`. It also affects multiple uses of the `Heap::extend` method. Version 0.10.2 contains a patch for the issue. As a workaround, ensure that the heap is only initialized with a size larger than `3 * size_of::usize` and that the `Heap::extend` method is only called with sizes larger than `2 * size_of::usize()`. Also, ensure that the total heap size is (and stays) a multiple of `2 * size_of::usize()`.

CVE-2022-36086 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: rust-osdev - linked-list-allocator version < 0.10.2

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Out-of-bound writes possible on `Heap` initialization and	github.com	CONFIRM github.com/rust-osdev/linked-list-

Heap::extend · Advisory · rust-osdev/linked-list-allocator · GitHub

text/html

allocator/security/advisories/GHSA-xg8p-34w2-j49j

Merge pull request from GHSA-xg8p-34w2-j49j · rust-osdev/linked-list-allocator@013b075 · GitHub

github.comtext/html

MISC github.com/rust-osdev/linked-list-allocator/commit/013b0758643943e8df5b17bbb495460ff47e8bbf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rust-osdev	Linked-list-allocator	All	All	All	All
cpe:2.3:a:rust-osdev:linked-list-allocator:*:*:*:*:rust:*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-36086 : linked_list_allocator is an allocator usable for no_std systems. Prior to version 0.10.2, the heap... twitter.com/i/web/status/1...	2022-09-07 22:57:43
/r/netcve	CVE-2022-36086	2022-09-07 23:38:17

← Previous ID

Next ID →