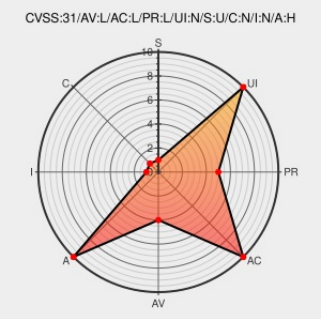
CVE-2022-23523

Published on: Not Yet Published

Last Modified on: 06/27/2023 02:59:00 PM UTC

CVE-2022-23523 - advisory for GHSA-52h2-m2cf-9jh6

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux-loader from Linux-loader Project contain the following vulnerability:

In versions prior to 0.8.1, the linux-loader crate uses the offsets and sizes provided in the ELF headers to determine the offsets to read from. If those offsets point beyond the end of the file this could lead to Virtual Machine Monitors using the `linux-loader` crate entering an infinite loop if the ELF header of the kernel they are loading was modified in a malicious manner. This issue has been addressed in 0.8.1. The issue can be mitigated by ensuring that only trusted kernel images are loaded or by verifying that the headers do not point beyond the end of the file.

CVE-2022-23523 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **rust-vmm** - **linux-loader** version **= < 0.8.1**

CVSS3 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
loader: x86_64: elf: Avoid reading beyond file end by likebreath · Pull Request #125 · rust-vmm/linux-loader · GitHub	github.com text/html	MISC github.com/rust-vmm/linux-loader/pull/125
Reading beyond EOF could lead to infinite loop · Advisory · rust-vmm/linux-loader · GitHub	github.com text/html	MISC github.com/rust-vmm/linux-loader/security/advisories/GHSA-52h2-m2cf-9jh6

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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linux-loader Project	Linux-loader	All	All	All	All

cpe:2.3:a:linux-loader_project:linux-loader:*:*:*:*:*:rust:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23523 : In versions prior to 0.8.1, the linux-loader crate uses the offsets and sizes provided in the ELF… twitter.com/i/web/status/1…	2022-12-13 08:02:21
@threatmeter	CVE-2022-23523 | linux-loader up to 0.8.0 infinite loop A vulnerability was found in linux-loader up to 0.8.0. It h… twitter.com/i/web/status/1…	2022-12-13 08:53:31
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-23523 - In versions prior to 0.8.1, the linux-loader crate uses the offsets a… twitter.com/i/web/status/1…	2022-12-13 08:53:37
/r/netcve	CVE-2022-23523	2022-12-13 09:39:25
/r/DailyCVE	CVE-2022-23523	2022-12-13 13:38:05

← Previous ID

Next ID→