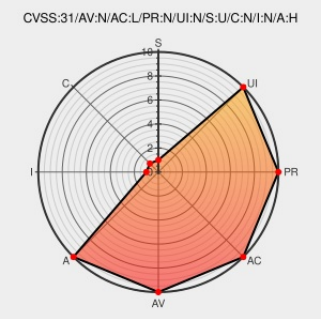
CVE-2020-27173

Published on: 10/15/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-27173

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



Certain versions of Vm-superio from Vm-superio Project contain the following vulnerability:

In vm-superio before 0.1.1, the serial console FIFO can grow to unlimited memory usage when data is sent to the input source (i.e., standard input). This behavior cannot be reproduced from the guest side. When no rate limiting is in place, the host can be subject to memory pressure, impacting all other VMs running on the same host.

CVE-2020-27173 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix for #17 - v0.1.1_release branch by andreeaflorescu · Pull Request #19 · rust-vmm/vm-superio · GitHub	Patch, Third Party Advisory, github.com	MISC github.com/rust-vmm/vm-superio/pull/19

	text/html	
Implementation of the serial console may allocate an unbounded amount of memory · Issue #17 · rust-vmm/vm-superio · GitHub	Third Party Advisory github.com text/html	MISC github.com/rust-vmm/vm-superio/issues/17

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	Vm-superio Project	Vm-superio	All	All	All	All
Application	Vm-superio Project	Vm-superio	All	All	All	All

cpe:2.3:a:vm-superio_project:vm-superio:*:*:*:*:*:*:*:*:

cpe:2.3:a:vm-superio_project:vm-superio:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→