

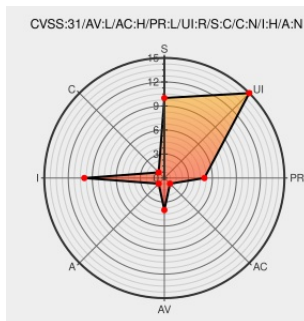


CVE-2020-15107

Published on: 07/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15107 - advisory for GHSA-7wjx-wcwg-w999

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openenclave](#) from [Openenclave](#) contain the following vulnerability:

In openenclave before 0.10.0, enclaves that use x87 FPU operations are vulnerable to tampering by a malicious host application. By violating the Linux System V Application Binary Interface (ABI) for such operations, a host app can compromise the execution integrity of some x87 FPU operations in an enclave. Depending on the FPU control

configuration of the enclave app and whether the operations are used in secret-dependent execution paths, this vulnerability may also be used to mount a side-channel attack on the enclave. This has been fixed in 0.10.0 and the current master branch. Users will need to recompile their applications against the patched libraries to be protected from this vulnerability.

CVE-2020-15107 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: openenclave - openenclave version < 0.10.0

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **1.2 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

PARTIAL

NONE

CVE References

Description	Tags	Link
x87 FPU operations in enclaves are vulnerable to ABI poisoning · Advisory · openenclave/openenclave · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/openenclave/openenclave/security/advisories/GHSA-7wjx-wcwg-w999

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	Openenclave	Openenclave	All	All	All	All
Application	Openenclave	Openenclave	All	All	All	All

cpe:2.3:a:openenclave:openenclave:*****:.*

cpe:2.3:a:openenclave:openenclave:*****:.*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →