

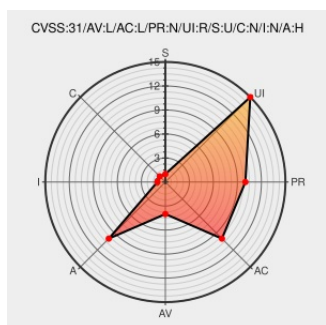


CVE-2021-36979

Published on: 07/20/2021 12:00:00 AM UTC

Last Modified on: 12/03/2021 01:48:00 PM UTC

CVE-2021-36979

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

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

Unicorn Engine 1.0.2 has an out-of-bounds write in `tb_flush_armeb` (called from `cpu_arm_exec_armeb` and `tcg_cpu_exec_armeb`).

CVE-2021-36979 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
30391 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	bugs.chromium.org text/html	MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=30391
oss-fuzz-vulns/OSV-2020-2305.yaml at main · google/oss-fuzz-vulns · GitHub	github.com text/html	MISC github.com/google/oss-fuzz-vulns/blob/main/vulns/unicorn/OSV-2020-2305.yaml

Add arm ite blocks samples from #853
(#1381) · unicorn-
engine/unicorn@bf1713d · GitHub

github.com
text/html

MISC github.com/unicorn-
engine/unicorn/commit/bf1713d9e011b55ca1f502a6779fc4722b4bb077

[SECURITY] Fedora 35 Update: unicorn-
1.0.3-1.fc35 - package-announce - Fedora
Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2021-53dd27bb86

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
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Unicorn-engine	Unicorn Engine	1.0.2	All	All	All

cpe:2.3:o:fedoraproject:fedora:35:*****:

cpe:2.3:a:unicorn-engine:unicorn_engine:1.0.2:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-36979 : Unicorn Engine 1.0.2 has an out-of-bounds write in tb_flush_armeb called from cpu_arm_exec_armeb... twitter.com/i/web/status/1...	2021-07-20 07:08:23
 @threatmeter	CVE-2021-36979 Unicorn Engine 1.0.2 has an out-of-bounds write in tb_flush_armeb (called from cpu_arm_exec_armeb an... twitter.com/i/web/status/1...	2021-07-21 07:50:31
 /r/netcve	CVE-2021-36979	2021-07-20 07:40:45

← Previous ID

Next ID →

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)