



CVE-2022-29694

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-29694
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-02 14:15:00 UTC
Updated	2022-06-13 13:47:00 UTC
Description	Unicorn Engine v2.0.0-rc7 and below was discovered to contain a NULL pointer dereference via qemu_ram_free.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Unicorn-engine	Unicorn Engine	All	All	All	All
Application	Unicorn-engine	Unicorn Engine	2.0.0	-	All	All
Application	Unicorn-engine	Unicorn Engine	2.0.0	rc1	All	All
Application	Unicorn-engine	Unicorn Engine	2.0.0	rc2	All	All
Application	Unicorn-engine	Unicorn Engine	2.0.0	rc3	All	All
Application	Unicorn-engine	Unicorn Engine	2.0.0	rc4	All	All
Application	Unicorn-engine	Unicorn Engine	2.0.0	rc5	All	All
Application	Unicorn-engine	Unicorn Engine	2.0.0	rc6	All	All

References

Reference	Source
Fix https://github.com/unicorn-engine/unicorn/issues/1588 by liyansong2018 · Pull Request #1593 · unicorn-engine/unicorn · GitHub	MISC
Fix https://github.com/unicorn-engine/unicorn/issues/1588 by liyansong2018 · Pull Request #1593 · unicorn-engine/unicorn · GitHub	MISC
Simple Analysis of Software Virtualization of Memory in Unicorn Engine - Violent Binary	MISC
Null pointer dereference in `qemu_ram_free` when HVA malloc fails · Issue #1588 · unicorn-engine/unicorn · GitHub	MISC
Fix crash when mapping a big memory and calling uc_close · unicorn-engine/unicorn@3d3deac · GitHub	MISC
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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