CVE-2021-44078

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-44078
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-26 05:15:00 UTC
Updated	2022-01-07 18:29:00 UTC
Description	An issue was discovered in split_region in uc.c in Unicorn Engine before 2.0.0-rc5. It allows local attackers to escape the sa

Risk And Classification

Problem Types: CWE-697

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2021-4407 reference · GitHub	MISC	gist.github.com	
Comparing 2.0.0-rc4...2.0.0-rc5 · unicorn-engine/unicorn · GitHub	CONFIRM	github.com	
CTF/UnicornsAisle.pdf at master · jwang-a/CTF · GitHub	MISC	github.com	
Fix wrong offset used in split_region · unicorn-engine/unicorn@c733bba · GitHub	MISC	github.com	
Version history – Unicorn – The Ultimate CPU emulator	MISC	www.unicorn-engine.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

691108 Free Berkeley Software Distribution (FreeBSD) Security Update for py39 (17083017-d993-43eb-8aaf-7138f4486d1c)