



CVE-2023-28502

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

Summary

CVE	CVE-2023-28502
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-29 21:15:00 UTC
Updated	2023-04-12 19:15:00 UTC
Description	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Rocketsoftware	Unidata	All	All	All	All
Application	Rocketsoftware	Universe	All	All	All	All
Application	Rocketsoftware	Universe	All	All	All	All

References

Reference	Source	Link	Tags
Rocket Software Unidata 8.2.4 Build 3003 Buffer Overflow ~ Packet Storm	MISC	packetstormsecurity.com	
Multiple Vulnerabilities in Rocket Software UniData's UniRPC server (Fixed) Rapid7 Blog	MISC	www.rapid7.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)