



CVE-2022-28365

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-28365
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-09 17:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	Reprise License Manager 14.2 is affected by an Information Disclosure vulnerability via a GET request to /goforms/r/rlminfo.

Risk And Classification

Problem Types: CWE-425

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Reprisesoftware	Reprise License Manager	14.2	All	All	All

References

Reference	Source	Link	Tags
www.reprisesoftware.com/RELEASE_NOTES	CONFIRM	www.reprisesoftware.com	
Reprise License Manager 14.2 Cross Site Scripting / Information Disclosure ≈ Packet Storm	MISC	packetstormsecurity.com	
Reprise Software Software License Management Concurrent Licensing	MISC	www.reprisesoftware.com	
Full Disclosure: Multiple Vulnerabilities in Reprise License Manager 14.2	MISC	seclists.org	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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

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](#)