



CVE-2022-41441

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

Summary

CVE	CVE-2022-41441
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-20 15:15:00 UTC
Updated	2023-03-28 17:15:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in ReQlogic v11.3 allow attackers to execute arbitrary web scripts or HTML

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Reqlogic	Reqlogic	11.3	All	All	All

References

Reference	Source	Link	Tags
ReQlogic 11.3 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com	
ReQlogic v11.3 – Unauthenticated Reflected Cross-Site Scripting (XSS) Okan KURTULUS	MISC	okankurtulus.com.tr	
Microsoft Dynamics ERP End-to-End eProcurement Solution ReQlogic	MISC	reqlogic.com	
Microsoft Dynamics ERP End-to-End eProcurement Solution ReQlogic	MISC	reqlogic.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.

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