



CVE-2023-42814

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

Summary

CVE	CVE-2023-42814
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-13 21:15:00 UTC
Updated	2023-11-14 19:15:00 UTC
Description	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference
fix: address vulnerability issues in notary implementations (#8428) · kyverno/kyverno@fec2992 · GitHub
Check payload counts and limits for image verification data returned from registries by vishal-chdhry · Pull Request #8428 · kyverno/kyverno ·
Denial of service from malicious image manifest · Advisory · kyverno/kyverno · GitHub
Added `fetchAttestations` method to notaryV2 implimentation (#6800) · kyverno/kyverno@80d139b · GitHub
CVE Program record
NVD vulnerability detail

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](#)

