



CVE-2022-29161

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

Summary

CVE	CVE-2022-29161
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-06 00:15:00 UTC
Updated	2023-07-21 16:42:00 UTC
Description	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The XWiki Crypto API wi

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xwiki	Xwiki	All	All	All	All

References

Reference	Source
XWIKI-19676: Update the RSA Crypto script service to use SHA256 inste... · xwiki/xwiki-platform@26728f3 · GitHub	MISC
[XWIKI-19676] Update the RSA Crypto script service to use SHA256 instead of SHA1 for certificate signature - XWiki.org JIRA	MISC
Crypto script service uses hashing algorithm SHA1 with RSA for certificate signature · Advisory · xwiki/xwiki-platform · GitHub	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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