CVE-2020-5229

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-5229
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-30 20:15:00 UTC
Updated	2020-02-05 20:52:00 UTC
Description	Opencast before 8.1 stores passwords using the rather outdated and cryptographically insecure MD5 hash algorithm. Furth

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apereo	Opencast	All	All	All	All
Application	Apereo	Opencast	All	All	All	All

References

Reference	Source	Link	Tags
Replace MD5 with bcrypt for password hashing · opencast/opencast@32bfbe5 · GitHub	MISC	github.com	Patch
Password Hashing: Do not use MD5 · Advisory · opencast/opencast · GitHub	CONFIRM	github.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983115 Java (maven) Security Update for org.opencastproject:opencast-common-jpa-impl (GHSA-h362-m8f2-5x7c)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report