



CVE-2023-31581

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-31581
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2023-10-31 15:09:00 UTC
Description	Dromara Sureness before v1.0.8 was discovered to use a hardcoded key.

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dromara	Sureness	All	All	All	All

References

Reference	Source	Link
Using hardcoded cryptographic key when creating and verifying Json Web Token. · Issue #164 · dromara/sureness · GitHub	MISC	github.com
github.com/xubowenW/JWTissues/blob/main/sureness%20secure%20issues.md	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995764 Java (Maven) Security Update for com.usthe.sureness:sureness-core (GHSA-3j2f-58rq-g6p7)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)