



CVE-2023-43961

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

Summary

CVE	CVE-2023-43961
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2023-11-01 16:16:00 UTC
Description	An issue in Dromara SaToken version 1.3.50RC and before when using Spring dynamic controllers, a specially crafted request can bypass the authorization mechanism and access unauthorized resources.

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dromara	Sa-token	All	All	All	All

References

Reference

SaToken and Spring's differential handling of URLs raises authorization bypass vulnerabilities (SaToken和Spring对uri处理的差异化引发的越权)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995762](#) Java (Maven) Security Update for cn.dev33:sa-token-core (GHSA-w9vh-hv5g-7wmr)

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](#)