CVE-2023-32694

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

Summary

CVE	CVE-2023-32694
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-25 15:15:00 UTC
Updated	2023-06-01 17:21:00 UTC
Description	Saleor Core is a composable, headless commerce API. Saleor's `validate_hmac_signature` function is vulnerable to timing

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Add webhooks logic · saleor/saleor@1328274 · GitHub	MISC	github.com	
Non-constant time HMAC comparison in Adyen plugin · Advisory · saleor/saleor · GitHub	MISC	github.com	
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.

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

Free CVE JSON API cve.report/api

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