



CVE-2020-15085

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

Summary

CVE	CVE-2020-15085
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-30 17:15:00 UTC
Updated	2020-07-28 15:45:00 UTC
Description	In Saleor Storefront before version 2.10.3, request data used to authenticate customers was inadvertently cached in the browser.

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
saleor-storefront/CHANGELOG.md at master · mirumee/saleor-storefront · GitHub	MISC	github.com	Release
Merge pull request from GHSA-4279-h39w-2jqm · mirumee/saleor-storefront@7c331e1 · GitHub	MISC	github.com	Patch, Tr
Client caching login operation with plaintext password · Advisory · mirumee/saleor-storefront · GitHub	CONFIRM	github.com	Third Par
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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