



Saleor Affected by Denial of Service via Unbounded GraphQL Query Batching

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

Summary

CVE	CVE-2026-33756
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 18:26:00 UTC
Updated	2026-04-08 21:26:13 UTC
Description	Saleor is an e-commerce platform. From 2.0.0 to before 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118, Saleor supports query b

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security-advisories@github.com

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.000810000 probability, percentile 0.239760000 (date 2026-04-09)

Problem Types: CWE-770 | CWE-770 CWE-770: Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Saleor	Saleor	affected >= 2.0.0, < 3.20.118	Not specified
CNA	Saleor	Saleor	affected >= 3.21.0-a.0, < 3.21.54	Not specified
CNA	Saleor	Saleor	affected >= 3.22.0-a.0, < 3.22.47	Not specified
CNA	Saleor	Saleor	affected >= 3.23.0-a.0, < 3.23.0a3	Not specified

References

Reference	Source	Link	Tags
github.com/saleor/saleor/commit/f0371bdd4cafcc841f1a9e7049cead6133bf7464	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/d6a94e95bd77f3f733fa66afd1b1ac72e863ca2a	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/cdb66da97abb7c86939e384914cd8d9194f378e8	security-advisories@github.com	github.com	
github.com/saleor/saleor/security/advisories/GHSA-24jw-f244-qfpp	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/7be352fa8c35875d6e66d36493ca7c14c101bd64	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/e42aa4d6e588982e78942b033af051c8ec8f43fa	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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