Improper restriction of the scope of accessible objects in Thymeleaf expressions

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

Summary

CVE	CVE-2026-40477
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 22:16:33 UTC
Updated	2026-04-17 22:16:33 UTC
Description	Thymeleaf is a server-side Java template engine for web and standalone environments. Versions 3.1.3.RELEASE and prior

Risk And Classification

Primary CVSS: v3.1 9 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-917 | CWE-1336 | CWE-917 CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') | CWE-1336 CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9	CRITICAL	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Thymeleaf	Thymeleaf	affected < 3.1.4.RELEASE	Not specified
CNA	Thymeleaf	Org.thymeleafthymeleaf-spring5	affected < 3.1.4.RELEASE	Not specified
CNA	Thymeleaf	Org.thymeleafthymeleaf-spring6	affected < 3.1.4.RELEASE	Not specified

References

Reference	Source	Link	Tags
github.com/thymeleaf/thymeleaf/security/advisories/GHSA-r4v4-5mwr-2fwr	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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