snyk | SECURITY

Incorrect Control Flow Scoping

Affecting @tootallnate/once package, versions

<2.0.1 >=3.0.0 <3.0.1

INTRODUCED: 2 FEB 2026 CVE-2026-3449 CWE-705 FIRST ADDED BY SNYK

How to fix?

Upgrade `@tootallnate/once` to version 2.0.1, 3.0.1 or higher.

Overview

Affected versions of this package are vulnerable to Incorrect Control Flow Scoping in promise resolving when `AbortSignal` option is used. The Promise remains in a permanently pending state after the signal is aborted, causing any `await` or `.then()` usage to hang indefinitely. This can cause a control-flow leak that can lead to stalled requests, blocked workers, or degraded application availability.

References

- GitHub Commit
- GitHub Issue

CVSS Base Scores

version 4.0 | version 3.1

Snyk RECOMMENDED 4.8 MEDIUM

Attack Vector (AV)	Local	Confidentiality (VC)	None	Confidentiality (SC)	None
Attack Complexity (AC)	Low	Integrity (VI)	None	Integrity (SI)	None
Attack Requirements (AT)	None	Availability (VA)	Low	Availability (SA)	None
Privileges Required (PR)	Low				

Severity RECOMMENDED

CVSS assessment by Snyk's Security Team. Learn more

Threat Intelligence

Exploit Maturity PROOF OF CONCEPT

EPSS 0.01% (4th percentile)

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID SNYK-JS-TOOTALLNATEONCE-15250612

User Interaction (UI)	None

Published 2 Mar 2026

Disclosed 2 Feb 2026

Credit Nanak Singh Khurana

Report a new vulnerability

Found a mistake?