



CVE-2023-26141

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

Summary

CVE	CVE-2023-26141
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-14 05:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	Versions of the package sidekiq before 7.1.3 are vulnerable to Denial of Service (DoS) due to insufficient checks in the dashboard.

Risk And Classification

Problem Types: CWE-345

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Contribsys	Sidekiq	All	All	All	All

References

Reference	Source	Link	Tags
Validate page refresh interval to ensure a minimum amount of delay · sidekiq/sidekiq@62c90d7 · GitHub	MISC	github.com	
Sidekiq DoS · GitHub	MISC	gist.github.com	
github.com/sidekiq/sidekiq/blob/6-x/web/assets/javascripts/dashboard.js%...	MISC	github.com	
Denial of Service (DoS) in sidekiq CVE-2023-26141 Snyk	MISC	security.snyk.io	
MISC:https://github.com/sidekiq/sidekiq/blob/6-x/web/assets/javascripts/dashboard.js%23L6	MITRE	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[242923](#) Red Hat Update for Satellite 6.14.2 (RHSA-2024:0797)

[995284](#) Rubygems (Rubygems) Security Update for sidekiq (GHSA-3qc2-v3hp-6cv8)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)