



CVE-2017-12097

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

Summary

CVE	CVE-2017-12097
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-19 20:29:00 UTC
Updated	2023-01-28 01:34:00 UTC
Description	An exploitable cross site scripting (XSS) vulnerability exists in the filter functionality of the delayed_job_web rails gem version 1.4.0. An attacker can inject a malicious payload into the filter functionality, which can be executed by the application. This vulnerability can be exploited to perform a cross site scripting (XSS) attack, which can be used to steal sensitive information or perform other malicious actions.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Delayed Job Web Project	Delayed Job Web	1.4	All	All	All
Application	Delayed Job Web Project	Delayed Job Web	1.4	All	All	All

References

Reference	Source	Link	Tags
RubyGems 'delayed_job_web' CVE-2017-12097 Cross Site Scripting Vulnerability	BID	www.securityfocus.com	Third Party
TALOS-2017-0449 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	www.talosintelligence.com	Exploit, Advisory
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.

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