

CVE-2016-0752

Rails Ruby on Rails Directory Traversal Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

Directory traversal vulnerability in Action View in Ruby on Rails before 3.2.22.1, 4.0.x and 4.1.x before 4.1.14.1, 4.2.x before 4.2.5.1, and 5.x before 5.0.0.beta1.1 allows remote attackers to read arbitrary files by leveraging an application's unrestricted use of the render method and providing a .. (dot dot) in a pathname.

EVRS 83/100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.955 99.87th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.955 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
actionview	≥ 4.0.0, ≤ 4.1.14.0	4.1.14.1	GitHub
actionview	≥ 4.2.0, ≤ 4.2.5.0	4.2.5.1	GitHub
actionpack	≥ 4.0.0, ≤ 4.1.14.0	4.1.14.1	GitHub
actionpack	≥ 4.2.0, ≤ 4.2.5.0	4.2.5.1	GitHub
actionpack	< 3.2.22.1	3.2.22.1	GitHub
rails	< 3.2.22.1 ≥ 4.0.0 < 4.1.14.1 ≥ 4.2.0 < 4.2.5.1 5.0.0	no fixed version listed	NVD
software collections	1.0	no fixed version listed	NVD
leap	42.1	no fixed version listed	NVD
opensuse	13.2	no fixed version listed	NVD
linux enterprise module for containers	12	no fixed version listed	NVD
debian linux	8.0	no fixed version listed	NVD

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2016-0752

GitHub advisory github.com/advisories/GHSA-xrr4-p6fq-hjg7

Current data evulnable.com/vulnerability-management/cve/CVE-2016-0752

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-0333

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.