

CVE-2015-5317

Jenkins User Interface (UI) Information Disclosure Vulnerability

CISA KEV since May 12, 2023

Actively exploited

The Fingerprints pages in Jenkins before 1.638 and LTS before 1.625.2 might allow remote attackers to obtain sensitive job and build name information via a direct request.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.230 97.7th percentile · FIRST	CISA DEADLINE Jun 2, 2023 KEV since 2023 · 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	0.230 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
org.jenkins-ci.main:jenkins-core	< 1.625.2	1.625.2	GitHub
org.jenkins-ci.main:jenkins-core	≥ 1.626, < 1.638	1.638	GitHub
jenkins	≤ 1.637 ≤ 1.625.1	after 1.637 · after 1.625.1	NVD
openshift	2.0 ≤ 3.1	after 3.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-8pqx-3rxx-f5pm

jenkins.io jenkins.io/security/advisory/2015-11-11/cisa.gov/known-exploited-vulnerabilities-catalog

CISA KEV evulnable.com/vulnerability-management/cve/CVE-2015-5317

Additional guidance wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2015-11-11
NVD nvd.nist.gov/vuln/detail/CVE-2015-5317
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2015-5288

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