CVE-2025-31725 Detail

RECEIVED

This CVE record has recently been published to the CVE List and has been included within the NVD dataset.

Description

Jenkins monitor-remote-job Plugin 1.0 stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD
Base Score: N/A
NVD assessment not yet provided.

ADP: CISA-ADP
Base Score: 5.5 MEDIUM
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource

Hyperlink	Resource
https://www.jenkins.io/security/advisory/2025-04-02/#SECURITY-3539	

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-284	Improper Access Control	CISA-ADP

Change History

2 change records found show changes

QUICK INFO

CVE Dictionary Entry:

CVE-2025-31725

NVD Published Date:

04/02/2025

NVD Last Modified:

04/03/2025

Source:

Jenkins Project