National Cyber Security Centre

2401260161-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Jenkins Project Jenkins (CVE-2024-23897)

Friday 26th January, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-01-24T18:15:00
Vendor: Jenkins Project
Product: Jenkins
CVE ID: CVE-2024-23897
CVSS3.0 Score[1]**:** not yet provided
EPSS[2]**:** not yet provided
Summary: Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

More information related to this issue can be found at the following link(s):
https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3314

Products Affected

- Jenkins Project Jenkins
- Jenkins weekly up to and including 2.441,
- Jenkins LTS up to and including 2.426.2

Impact

Present in CISA Known Exploited Vulnerability(KEV)[3] **catalog:** NO

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Jenkins Project.

Additional recommendations and mitigation's for CVE-2024-23897 can be found in the respective link(s) below:
https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3314

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie