



CVE-2023-24422

Published on: Not Yet Published

Last Modified on: 02/04/2023 02:08:00 AM UTC

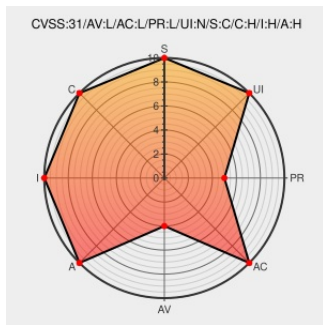
CVE-2023-24422

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Script Security](#) from [Jenkins](#) contain the following vulnerability:

A sandbox bypass vulnerability involving map constructors in Jenkins Script Security Plugin 1228.vd93135a_2fb_25 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM.

CVE-2023-24422 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Jenkins Project - Jenkins Script Security Plugin](#) version <= 1228.vd93135a_2fb_25

Affected Vendor/Software: [Jenkins Project - Jenkins Script Security Plugin](#) version ! 1175.1180.v36a_3fb_2dec9c

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Jenkins Security Advisory 2023-01-24	www.jenkins.io text/html	MISC www.jenkins.io/security/advisory/2023-01-24/#SECURITY-3016

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites 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 websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

241340 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:1655)

770184 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:1655)

Exploit/POC from Github



A sandbox bypass vulnerability involving map constructors in Jenkins Script Security Plugin 1228.vd93135a_2fb_25 and ...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Script Security	All	All	All	All
cpe:2.3:a:jenkins:script_security:*:*:*:*:jenkins:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RedPacketSec	Jenkins Script Security Plugin code execution CVE-2023-24422 - redpacketsecurity.com/jenkins-script... #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2023-01-26 10:01:42
 @CVEreport	CVE-2023-24422 : A sandbox bypass vulnerability involving map constructors in Jenkins Script Security Plugin 1228.v... twitter.com/i/web/status/1...	2023-01-26 22:10:11

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)