



CVE-2019-10355

Published on: 07/31/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:39 PM UTC

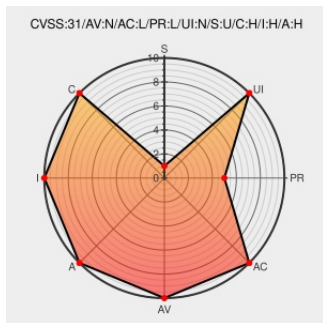
CVE-2019-10355

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.61 and earlier related to the handling of type casts allowed attackers to execute arbitrary code in sandboxed scripts.

CVE-2019-10355 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 **1.61 and earlier**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Jenkins Security Advisory 2019-07-31	Vendor Advisory jenkins.io	jenkins.io/security/advisory/2019-07-31/#SECURITY-1465%20(1)

	jenkins text/html	CVE-2019-0294
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2019:2651
oss-security - Multiple vulnerabilities in Jenkins plugins	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20190731 Multiple vulnerabilities in Jenkins plugins
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2019:2594
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2019:2662
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 .		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Script Security	All	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
cpe:2.3:a:jenkins:script_security:*:*:*:*:*:jenkins:*:*						
cpe:2.3:a:redhat:openshift_container_platform:3.11:*:*:*:*:*:						
cpe:2.3:a:redhat:openshift_container_platform:4.1:*:*:*:*:*:						
cpe:2.3:a:redhat:openshift_container_platform:3.11:*:*:*:*:*:						
cpe:2.3:a:redhat:openshift_container_platform:4.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)