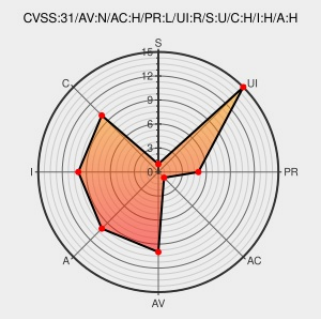
CVE-2020-27833

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:53 PM UTC

CVE-2020-27833

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openshift Container Platform from Redhat contain the following vulnerability:

A Zip Slip vulnerability was found in the oc binary in openshift-clients where an arbitrary file write is achieved by using a specially crafted raw container image (.tar file) which contains symbolic links. The vulnerability is limited to the command `oc image extract`. If a symbolic link is first created pointing within the tarball, this allows further symbolic links to bypass the existing path check. This flaw allows the tarball to create links outside the tarball's parent directory, allowing for executables or configuration files to be overwritten, resulting in arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions up to and including openshift-clients-4.7.0-202104250659.p0.git.95881af are affected.

CVE-2020-27833 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
1905945 – (CVE-2020-27833) CVE-2020-27833 openshift/oc: zip slip - arbitrary file write vulnerability / arbitrary code execution using a specially crafted container image	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1905945
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	CONFIRM access.redhat.com/security/cve/CVE-2020-27833

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for exploiting CVE-2020-27833

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift Container Platform	All	All	All	All

cpe:2.3:a:redhat:openshift_container_platform:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-27833 : A Zip Slip vulnerability was found in the oc binary in openshift-clients where an arbitrary file w… twitter.com/i/web/status/1…	2021-05-14 21:03:50
/r/netcve	CVE-2020-27833	2021-05-14 21:41:36

← Previous ID

Next ID→