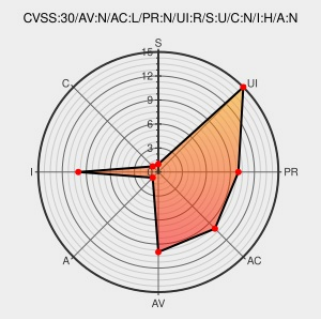
CVE-2018-1103

Published on: 06/12/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:32 PM UTC

CVE-2018-1103

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



Certain versions of Source-to-image from Redhat contain the following vulnerability:

Openshift Enterprise source-to-image before version 1.1.10 is vulnerable to an improper validation of user input. An attacker who could trick a user into using the command to copy files locally, from a pod, could override files outside of the target directory of the command.

CVE-2018-1103 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Openshift Enterprise** - **unsanitized paths in tar.go** version **source-to-image 1.1.10**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
1563993 – (CVE-2018-1103) CVE-2018-1103 source-to-image: Unsanitized paths in tar.go:ExtractTarStreamFromTarReader() allow malicious containers to overwrite files on the client machine	Issue Tracking, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-1103

overwrite files on the client machine

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	Redhat	Source-to-image	All	All	All	All
Application	Redhat	Source-to-image	All	All	All	All

cpe:2.3:a:redhat:source-to-image:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:source-to-image:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→