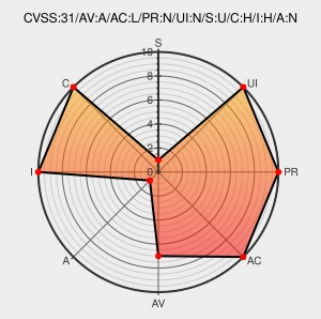
CVE-2021-36780

Published on: 12/17/2021 12:00:00 AM UTC

Last Modified on: 02/10/2023 02:30:00 AM UTC

CVE-2021-36780 - advisory for https://bugzilla.suse.com/show_bug.cgi?id=1191819

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



Certain versions of Longhorn from Linuxfoundation contain the following vulnerability:

A Missing Authentication for Critical Function vulnerability in longhorn of SUSE Longhorn allows attackers to connect to a longhorn-engine replica instance granting it the ability to read and write data to and from a replica that they should not have access to. This issue affects: SUSE Longhorn longhorn versions prior to 1.1.3; longhorn versions prior to 1.2.3v.

CVE-2021-36780 has been assigned by security@suse.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SUSE** - **Longhorn** version **< 1.1.3**

Affected Vendor/Software: **SUSE** - **Longhorn** version **< 1.2.3v**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 4.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Bug 1191819 – VUL-0: CVE-2021-36780: Unauthorized data access from replicas through vulnerable instance manager pods	bugzilla.suse.com text/html	CONFIRM bugzilla.suse.com/show_bug.cgi?id=1191819
Host operations allowed in privileged Longhorn managed pods · Advisory · longhorn/longhorn · GitHub	github.com text/html	CONFIRM github.com/longhorn/longhorn/security/advisories/GHSA-g358-m2wp-mhhx

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	Linuxfoundation	Longhorn	All	All	All	All

cpe:2.3:a:linuxfoundation:longhorn:*:*:*:*:*:*:*:*:

Discovery Credit

Dagan Henderson and Will Kline

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-36780 : A Improper Access Control vulnerability in longhorn of SUSE Longhorn allows attackers to connect t… twitter.com/i/web/status/1…	2021-12-17 09:00:43
/r/netcve	CVE-2021-36780	2021-12-17 09:38:30

← 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 registred 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