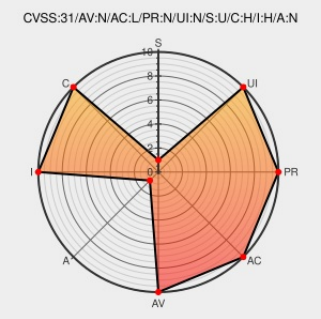
CVE-2021-32700

Published on: 06/22/2021 12:00:00 AM UTC

Last Modified on: 06/29/2021 06:56:00 PM UTC

CVE-2021-32700 - advisory for GHSA-f5qg-fqrw-v5ww

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



Certain versions of Ballerina from Ballerina contain the following vulnerability:

Ballerina is an open source programming language and platform for cloud application programmers. Ballerina versions 1.2.x and SL releases up to alpha 3 have a potential for a supply chain attack via MiTM against users. Http connections did not make use of TLS and certificate checking was ignored. The vulnerability allows an attacker to substitute or modify packages retrieved from BC thus allowing to inject malicious code into ballerina executables. This has been patched in Ballerina 1.2.14 and Ballerina SwanLake alpha4.

CVE-2021-32700 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **ballerina-platform** - **ballerina-lang** version **< 1.2.14**

Affected Vendor/Software: **ballerina-platform** - **ballerina-lang** version **< SL-alpha4**

CVSS3 Score: 7.4 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
Potential for a supply chain attack via MiTM against users · Advisory · ballerina-platform/ballerina-lang · GitHub	github.com text/html	CONFIRM github.com/ballerina-platform/ballerina-lang/security/advisories/GHSA-f5qg-fqrw-v5ww
Fix central connection · ballerina-platform/ballerina-lang@4609ffe · GitHub	github.com text/html	MISC github.com/ballerina-platform/ballerina-lang/commit/4609ffee1744ecd16aac09303b1783bf0a525816

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	Ballerina	Ballerina	All	All	All	All
Application	Ballerina	Swan Lake	alpha1	All	All	All
Application	Ballerina	Swan Lake	alpha2	All	All	All
Application	Ballerina	Swan Lake	alpha3	All	All	All

cpe:2.3:a:ballerina:ballerina:*:*:*:*:*:*:*:*:

cpe:2.3:a:ballerina:swan_lake:alpha1:*:*:*:*:*:*:*:

cpe:2.3:a:ballerina:swan_lake:alpha2:*:*:*:*:*:*:*:

cpe:2.3:a:ballerina:swan_lake:alpha3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32700 : Ballerina is an open source programming language and platform for cloud application programmers. B… twitter.com/i/web/status/1…	2021-06-22 19:31:56
/r/netcve	CVE-2021-32700	2021-06-22 20:41:28

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report