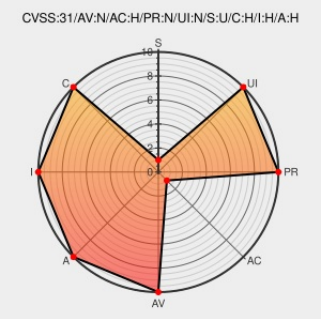
CVE-2021-37632

Published on: 08/05/2021 12:00:00 AM UTC

Last Modified on: 08/17/2021 03:00:00 PM UTC

CVE-2021-37632 - advisory for GHSA-f4r5-w453-2jx6

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



Certain versions of Config Lib from Config Lib Project contain the following vulnerability:

SuperMartijn642's Config Lib is a library used by a number of mods for the game Minecraft. The versions of SuperMartijn642's Config Lib between 1.0.4 and 1.0.8 are affected by a vulnerability and can be exploited on both servers and clients. Using SuperMartijn642's Config Lib, servers will send a packet to clients with the server's config values. In order to read `enum` values from the packet data, `ObjectInputStream#readObject` is used. `ObjectInputStream#readObject` will instantiate a class based on the input data. Since, the packet data is not validated before `ObjectInputStream#readObject` is called, an attacker can instantiate any class by sending a malicious packet. If a suitable class is found, the vulnerability can lead to a number of exploits, including remote code execution. Although the vulnerable packet is typically only send from server to client, it can theoretically also be send from client to server. This means both clients and servers running SuperMartijn642's Config Lib between 1.0.4 and 1.0.8 are vulnerable. The vulnerability has been patched in SuperMartijn642's Config lib 1.0.9. Both, players and server owners, should update to 1.0.9 or higher.

CVE-2021-37632 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SuperMartijn642** - **SuperMartijn642sConfigLib** version **>= 1.0.4, < 1.0.8**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Deserialization of Untrusted Data in com.supermartijn642.configlib.ConfigSyncPacket · Advisory · SuperMartijn642/SuperMartijn642sConfigLib · GitHub	github.com text/html	CONFIRM github.com/SuperMartijn642/SuperMartijn642sConfigLib/security/advisories/f4r5-w453-2jx6

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	Config Lib Project	Config Lib	All	All	All	All

cpe:2.3:a:config_lib_project:config_lib:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-37632 : SuperMartijn642's Config Lib is a library used by a number of mods for the game Minecraft. The ver… twitter.com/i/web/status/1…	2021-08-05 20:20:38

← Previous ID Next ID→