



# CVE-2023-28113

Published on: Not Yet Published

Last Modified on: 03/17/2023 04:04:00 AM UTC

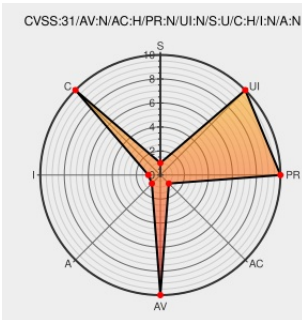
## CVE-2023-28113 - advisory for GHSA-cqvm-j2r2-hwpg

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Russh](#) from [Russh Project](#) contain the following vulnerability:

russh is a Rust SSH client and server library. Starting in version 0.34.0 and prior to versions 0.36.2 and 0.37.1, Diffie-Hellman key validation is insufficient, which can lead to insecure shared secrets and therefore breaks confidentiality. Connections between a russh client and server or those of a russh peer with some other misbehaving peer are most likely to be problematic. These may vulnerable to eavesdropping. Most other implementations reject such keys, so this is mainly an interoperability issue in such a case. This issue is fixed in versions 0.36.2 and 0.37.1

CVE-2023-28113 has been assigned by [security-advisories@github.com](#) to track the vulnerability

Affected Vendor/Software: [warp-tech](#) - **russh** version  $\geq$  0.34.0

Affected Vendor/Software: [warp-tech](#) - **russh** version  $<$  0.36.2

Affected Vendor/Software: [warp-tech](#) - **russh** version  $\geq$  0.37.0

Affected Vendor/Software: [warp-tech](#) - **russh** version  $<$  0.37.1

## CVE References

Description	Tags	Link
Release v0.36.2 · warp-tech/russh · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	<a href="#">MISC github.com/warp-tech/russh/releases/tag/v0.36.2</a>
Release v0.37.1 · warp-tech/russh · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	<a href="#">MISC github.com/warp-tech/russh/releases/tag/v0.37.1</a>
russh/groups.rs at master · warp-tech/russh · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	<a href="#">MISC github.com/warp-tech/russh/blob/master/russh/src/kex/dh/groups.rs#L72-L76</a>
russh may use insecure Diffie-Hellman keys · Advisory · warp-tech/russh · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	<a href="#">CONFIRM github.com/warp-tech/russh/security/advisories/GHSA-cqvm-j2r2-hwpg</a>
GHSA-cqvm-j2r2-hwpg validate DH key range · warp-tech/russh@d831a37 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	<a href="#">MISC github.com/warp-tech/russh/commit/d831a3716d3719dc76f091fcea9d94bd4ef97c6e</a>

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](mailto: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	<a href="#">Russh Project</a>	<a href="#">Russh</a>	All	All	All	All
Application	<a href="#">Russh Project</a>	<a href="#">Russh</a>	0.37.0	-	All	All
Application	<a href="#">Russh Project</a>	<a href="#">Russh</a>	0.37.0	beta1	All	All

cpe:2.3:a:russh\_project:russh:\*:\*:\*:\*:rust:\*:\*:

cpe:2.3:a:russh\_project:russh:0.37.0:-:\*:\*:\*:rust:\*:\*:

cpe:2.3:a:russh\_project:russh:0.37.0:beta1:\*:\*:\*:rust:\*:\*:

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28113 : russh is a Rust SSH client and server library. Starting in version 0.34.0 and prior to versions 0... <a href="#">twitter.com/i/web/status/1...</a>	2023-03-16 21:15:39
/r/netcve	<a href="#">CVE-2023-28113</a>	2023-03-16 21:38:55

[← 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 registered 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](#)