

# CVE-2021-36368



|                    |  |
|--------------------|--|
| <b>Name</b>        | CVE-2021-36368   |
| <b>Description</b> | An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without <code>-oLogLevel=verbose</code> , and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed." |
| <b>Source</b>      | <a href="#">CVE</a> (at <a href="#">NVD</a> ; <a href="#">CERT</a> , <a href="#">ENISA</a> , <a href="#">LWN</a> , <a href="#">oss-sec</a> , <a href="#">fulldisc</a> , <a href="#">Debian ELTS</a> , <a href="#">Red Hat</a> , <a href="#">Ubuntu</a> , <a href="#">Gentoo</a> , <a href="#">SUSE bugzilla/CVE</a> , <a href="#">GitHub advisories/code/issues</a> , <a href="#">web search</a> , <a href="#">more</a> )  |

## Vulnerable and fixed packages

The table below lists information on source packages.

| Source Package                | Release             | Version            | Status     |
|-------------------------------|---------------------|--------------------|------------|
| <a href="#">openssh (PTS)</a> | bullseye            | 1:8.4p1-5+deb11u3  | vulnerable |
|                               | bullseye (security) | 1:8.4p1-5+deb11u7  | vulnerable |
|                               | bookworm            | 1:9.2p1-2+deb12u10 | fixed      |
|                               | bookworm (security) | 1:9.2p1-2+deb12u9  | fixed      |
|                               | trixie              | 1:10.0p1-7+deb13u4 | fixed      |
|                               | trixie (security)   | 1:10.0p1-7+deb13u2 | fixed      |
|                               | forky               | 1:10.3p1-2         | fixed      |
|                               | sid                 | 1:10.3p1-4         | fixed      |

The information below is based on the following data on fixed versions.

| Package                 | Type   | Release    | Fixed Version | Urgency     | Origin | Debian Bugs |
|-------------------------|--------|------------|---------------|-------------|--------|-------------|
| <a href="#">openssh</a> | source | (unstable) | 1:8.9p1-1     | unimportant |        |             |

## Notes

[https://bugzilla.mindrot.org/show\\_bug.cgi?id=3316](https://bugzilla.mindrot.org/show_bug.cgi?id=3316)

<https://docs.ssh-mitm.at/trivialauth.html>

Search for package or bug name:   [Reporting problems](#)