CVE-2015-8325

Name	CVE-2015-8325
Description	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.
Source	CVE (at NVD; CERT, ENISA, LWN, oss-sec, fulldisc, Debian ELTS, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, GitHub advisories/code/issues, web search, more)
References	DSA-3550-1

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
openssh (PTS)	bullseye	1:8.4p1-5+deb11u3	fixed
	bullseye (security)	1:8.4p1-5+deb11u7	fixed
	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, 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
openssh	source	wheezy	1:6.0p1-4+deb7u4		DSA-3550-1	
openssh	source	jessie	1:6.7p1-5+deb8u2		DSA-3550-1	
openssh	source	(unstable)	1:7.2p2-3			

Notes

Upstream fix: https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7f

Search for package or bug name: Go Reporting problems

Home - Debian Security - Source (Git)