

Your submission was sent successfully! [Close](#)

Thank you for contacting us. A member of our team will be in touch shortly. [Close](#)

You have successfully unsubscribed! [Close](#)

Thank you for signing up for our newsletter!

In these regular emails you will find the latest updates about Ubuntu and upcoming events where you can meet our team. [Close](#)

Your preferences have been successfully updated. [Close notification](#)

Please try again or [file a bug report. <https://github.com/canonical/ubuntu.com/issues/new?template=ISSUE_TEMPLATE.yaml>](https://github.com/canonical/ubuntu.com/issues/new?template=ISSUE_TEMPLATE.yaml) [Close](#)

CVE-2015-8325

Publication date 30 April 2016

Last updated 25 August 2025

Ubuntu priority

Low

[Why this priority?](#)

Cvss 3 Severity Score

7.8 · High

[Score breakdown](#)

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.

[Read the notes from the security team](#)

Show unmaintained releases

Status

Package	Ubuntu Release	Status
openssh	17.04 zesty	Not affected
	16.10 yakkety	Not affected
	16.04 LTS xenial	Not affected
	15.10 wily	Fixed 1:6.9p1-2ubuntu0.2

We use cookies and similar methods to recognize visitors and remember preferences. We also use them to measure campaign effectiveness and analyze traffic on our websites. By selecting 'Accept', you consent to the use of these methods by us and trusted third parties. For further details or to change your consent choices at any time see our [cookie policy <https://canonical.com/legal/data-privacy?cp=hide#cookies>](https://canonical.com/legal/data-privacy?cp=hide#cookies).

[Manage your tracker settings](#)

Accept all

Notes

[tyhicks <https://launchpad.net/~tyhicks>](https://launchpad.net/~tyhicks)

Ubuntu is not affected in the default configuration since UseLogin is disabled in sshd_config

Patch details

For informational purposes only. We recommend not to cherry-pick updates. [How can I get the fixes?](#)

Package	Patch details
openssh	<ul style="list-style-type: none"> Upstream: ?id=85b <https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755>

Severity score breakdown

Parameter	Value
Base score	7.8 · High
Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity impact	High
Availability impact	High
Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References

- [MITRE <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8325>](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8325)
- [NVD <https://nvd.nist.gov/vuln/detail/CVE-2015-8325>](https://nvd.nist.gov/vuln/detail/CVE-2015-8325)
- [Launchpad <https://launchpad.net/bugs/cve/CVE-2015-8325>](https://launchpad.net/bugs/cve/CVE-2015-8325)
- [Debian <https://security-tracker.debian.org/tracker/CVE-2015-8325>](https://security-tracker.debian.org/tracker/CVE-2015-8325)

Related Ubuntu Security Notices (USN)

- [USN-2966-1 <https://usn.ubuntu.com/USN-2966-1>](https://usn.ubuntu.com/USN-2966-1)
- OpenSSH vulnerabilities
- 9 May 2016

Other references

We use cookies and similar methods to recognize visitors and remember preferences. We also use them to measure campaign effectiveness and analyze traffic on our websites. By selecting 'Accept', you consent to the use of these methods by us and trusted third parties. For further details or to change your consent choices at any time see our [cookie policy <https://canonical.com/legal/data-privacy?cp=hide#cookies>](https://canonical.com/legal/data-privacy?cp=hide#cookies) .

Access our resources on patching vulnerabilities

A guide to Infrastructure Hardening

→ Download

[A guide to Infrastructure Hardening](#)

Best practices to improve the security posture of your Linux-based infrastructure deployments

We use cookies and similar methods to recognize visitors and remember preferences. We also use them to measure campaign effectiveness and analyze traffic on our websites. By selecting 'Accept', you consent to the use of these methods by us and trusted third parties. For further details or to change your consent choices at any time see our [cookie policy](https://canonical.com/legal/data-privacy?cp=hide#cookies) <<https://canonical.com/legal/data-privacy?cp=hide#cookies>> .