



# CVE-2015-6565

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-6565
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-08-24 01:59:00 UTC
<b>Updated</b>	2022-12-13 12:15:00 UTC
<b>Description</b>	sshd in OpenSSH 6.8 and 6.9 uses world-writable permissions for TTY devices, which allows local users to cause a denial

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.8	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.9	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.8	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.9	All	All	All

## References

Reference	Source	Link
OpenSSH: Multiple vulnerabilities (GLSA 201512-04) — Gentoo Security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
OpenSSH TTY Permissions Let Local Users Cause Denial of Service Conditions - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>
<a href="http://www.openssh.com/txt/release-7.0">www.openssh.com/txt/release-7.0</a>	CONFIRM	<a href="http://www.openssh.com">www.openssh.com</a>
OpenSSH CVE-2015-6565 Local Security Bypass Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Document Display   HPE Support Center	CONFIRM	<a href="http://h20566.www2.hp.com">h20566.www2.hp.com</a>
Document Display   HPE Support Center	CONFIRM	<a href="http://h20566.www2.hp.com">h20566.www2.hp.com</a>
oss-security - Re: OpenSSH: CVE-2015-6565 (pty issue in 6.8-6.9) can lead to local privesc on Linux	MLIST	<a href="http://openwall.com">openwall.com</a>
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation - Linux local Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
<a href="http://cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf">cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf</a>	CONFIRM	<a href="http://cert-portal.siemens.com">cert-portal.siemens.com</a>
oss-security - Re: CVE request - OpenSSH 6.9 PAM privilege separation vulnerabilities	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>

Document Display   HPE Support Center	CONFIRM	<a href="https://h20566.www2.hpe.com">h20566.www2.hpe.co</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

**591280** Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

**690300** Free Berkeley Software Distribution (FreeBSD) Security Update for openssh (2920c449-4850-11e5-825f-c80aa9043978)

© [CVE.report](https://cve.report) 2026 |

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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)