



# CVE-2016-1908

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2016-1908
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-11 18:59:00 UTC
<b>Updated</b>	2022-12-13 12:15:00 UTC
<b>Description</b>	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	All	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	All	p2	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	6	-	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	7	-	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Li
[SECURITY] [DLA 1500-1] openssh security update	MLIST	lis
OpenSSH X11 Forwarding Flaw Lets Users Bypass Trust Restrictions - SecurityTracker	SECTRACK	w
Red Hat Customer Portal	REDHAT	rh
Red Hat Customer Portal	REDHAT	rh
oss-security - Re: Qualys Security Advisory - Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778	MLIST	op
OpenSSH: Multiple vulnerabilities (GLSA 201612-18) — Gentoo security	GENTOO	se
www.openssh.com/txt/release-7.2	CONFIRM	w
Oracle Linux Bulletin - April 2016	CONFIRM	w
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	ce
OpenSSH CVE-2016-1908 Security Bypass Vulnerability	BID	w
openssh.git - Portable OpenSSH	CONFIRM	ar
Bug 1298741 – CVE-2016-1908 openssh: possible fallback from untrusted to trusted X11 forwarding	CONFIRM	bu
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[38906](#) OpenSSH Improper Failed Cookie Generation Handling Vulnerability (CVE-2016-1908)

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

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](#)**