



# CVE-2014-2653

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

## Summary

<b>CVE</b>	CVE-2014-2653
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-03-27 10:55:00 UTC
<b>Updated</b>	2017-01-07 02:59:00 UTC
<b>Description</b>	The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the s

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.0	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.1	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.2	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.3	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.4	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.5	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.0	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.1	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.2	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.3	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.4	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	6.5	All	All	All
Application	<a href="#">Openbsd</a>	<a href="#">Openssh</a>	All	All	All	All

## References

Reference	Source
Support / Security / Advisories // MDVSA-2014:068   Mandriva	MANDRIVA

[SECURITY] Fedora 19 Update: openssh-6.2p2-8.fc19	FEDORA
Red Hat Customer Portal	REDHAT
Support / Security / Advisories // MDVSA-2015:095   Mandriva	MANDRIVA
Oracle Solaris Third Party Bulletin - October 2015	CONFIRM
OpenSSH Certificate Validation Security Bypass Vulnerability	BID
Red Hat Customer Portal	REDHAT
aix.software.ibm.com/aix/efixes/security/openssh_advisory4.asc	CONFIRM
#742513 - If server offers certificate, doesn't fall back to checking SSHFP records (CVE-2014-2653) - Debian Bug report logs	CONFIRM
Debian -- Security Information -- DSA-2894-1 openssh	DEBIAN
USN-2164-1: OpenSSH vulnerability   Ubuntu	UBUNTU
oss-security - CVE request: openssh client does not check SSHFP if server offers certificate	MLIST
[SECURITY] Fedora 20 Update: openssh-6.4p1-4.fc20	FEDORA
[security bulletin] HPSBUX03188 SSRT101487 rev.1 - HP-UX running HP Secure Shell, Remote Denial of S' - MARC	HP
Security Advisory SA59855 - SUSE update for openssh - Secunia	SECUNIA
Mageia Advisory: MGASA-2014-0166 - Updated openssh packages fix CVE-2014-2653	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)