Message-Id: <201403261424.04565.thijs@debian.org>
Date: Wed, 26 Mar 2014 14:24:04 +0100
From: Thijs Kinkhorst <thijs@...ian.org>
To: oss-security@...ts.openwall.com
Subject: CVE request: openssh client does not check SSHFP if server offers certificate

Hi,

A vulnerability in OpenSSH's ssh client has been reported in Debian's BTS:
https://bugs.debian.org/742513

If the ssh server offers a HostCertificate that the ssh client doesn't accept,
then the client doesn't then check the DNS for SSHFP records. This is a
security problem because it means that a malicious server can disable SSHFP-
checking by presenting a certificate. Note that users are still presented the
well-known "host verification prompt".

Given the prompt will and the still rather peripheral reliance on SSHFP, we
consider this an issue of low severity.

Please assign a CVE name for this issue.

Thanks,

Thijs Kinkhorst
Debian Security Team

Download attachment "signature.asc **" of type "**application/pgp-signature**" (491 bytes)**