Advisories » MGASA-2014-0166

Updated openssh packages fix CVE-2014-2653

Publication date: 08 Apr 2014
Modification date: 08 Apr 2014
Type: security
Affected Mageia releases : 3 , 4
CVE: CVE-2014-2653

Description

```
Updated openssh packages fix security vulnerability:

Matthew Vernon reported that if a SSH server offers a HostCertificate that
the ssh client doesn't accept, then the client doesn't check the DNS for
SSHFP records. As a consequence a malicious server can disable SSHFP-checking
by presenting a certificate (CVE-2014-2653).
```

References

- https://www.debian.org/security/2014/dsa-2894
- https://bugs.mageia.org/show_bug.cgi?id=13164
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2653

SRPMS

3/core

- openssh-6.1p1-4.3.mga3

4/core

- openssh-6.2p2-3.2.mga4