

[MDKSA-2006:207] – Updated bind packages fixes RSA signature verification vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-11/msg00256.html>

- *From:* security@xxxxxxxxxxxxx
 - *Date:* Tue, 14 Nov 2006 20:20:00 -0700
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Mandriva Linux Security Advisory MDKSA-2006:207
<http://www.mandriva.com/security/>

Package : bind
Date : November 14, 2006
Affected: 2006.0, 2007.0, Corporate 3.0, Corporate 4.0,
Multi Network Firewall 2.0

Problem Description:

The BIND DNS server is vulnerable to the recently-discovered OpenSSL RSA signature verification problem (CVE-2006-4339). BIND uses RSA cryptography as part of its DNSSEC implementation. As a result, to resolve the security issue, these packages need to be upgraded and for both KEY and DNSKEY record types, new RSASHA1 and RSAMD5 keys need to be generated using the "-e" option of dnssec-keygen, if the current keys were generated using the default exponent of 3.

You are able to determine if your keys are vulnerable by looking at the algorithm (1 or 5) and the first three characters of the Base64 encoded RSA key. RSAMD5 (1) and RSASHA1 (5) keys that start with "AQM", "AQN", "AQO", or "AQP" are vulnerable.

References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339>
<http://marc.theaimsgroup.com/?l=bind-announce&m=116253119512445>

[MDKSA-2006:207] – Updated bind packages fixes RSA signature verification vulnerability

Updated Packages:

Mandriva Linux 2006.0:

1035f92172986ed63ca035de0603a0fd 2006.0/i586/bind-9.3.1-4.2.20060mdk.i586.rpm
4f5949d85f13c68220f4f5f030f63849 2006.0/i586/bind-devel-9.3.1-4.2.20060mdk.i586.rpm
f201e05548b673268038e95225451085 2006.0/i586/bind-utils-9.3.1-4.2.20060mdk.i586.rpm
4f57cbdc960171c439223f5c20952460 2006.0/SRPMS/bind-9.3.1-4.2.20060mdk.src.rpm

Mandriva Linux 2006.0/X86_64:

83b6c31bef9e4df229e2fe5cf8c3aa2a 2006.0/x86_64/bind-9.3.1-4.2.20060mdk.x86_64.rpm
fb03e9a493645041816c206267a052f4 2006.0/x86_64/bind-devel-9.3.1-4.2.20060mdk.x86_64.rpm
f54babadfb3ec593563724208df1eaa 2006.0/x86_64/bind-utils-9.3.1-4.2.20060mdk.x86_64.rpm
4f57cbdc960171c439223f5c20952460 2006.0/SRPMS/bind-9.3.1-4.2.20060mdk.src.rpm

Mandriva Linux 2007.0:

6c282a7b5c3cfec534e2557926005bbf 2007.0/i586/bind-9.3.2-8.1mdv2007.0.i586.rpm
03390448f140777d62cdd76e50361526 2007.0/i586/bind-devel-9.3.2-8.1mdv2007.0.i586.rpm
7546dc98ff5e8061636a3a75d6b318fb 2007.0/i586/bind-utils-9.3.2-8.1mdv2007.0.i586.rpm
8be8a7d591971e760d1251bd75f97a6c 2007.0/SRPMS/bind-9.3.2-8.1mdv2007.0.src.rpm

Mandriva Linux 2007.0/X86_64:

c190d522505a16aa97891f525e0034a4 2007.0/x86_64/bind-9.3.2-8.1mdv2007.0.x86_64.rpm
594cacadac86db81b0c62a7380c6a3a2d 2007.0/x86_64/bind-devel-9.3.2-8.1mdv2007.0.x86_64.rpm
e827e65717615868896e43bcb4856f2d 2007.0/x86_64/bind-utils-9.3.2-8.1mdv2007.0.x86_64.rpm
8be8a7d591971e760d1251bd75f97a6c 2007.0/SRPMS/bind-9.3.2-8.1mdv2007.0.src.rpm

Corporate 3.0:

fa096b2fac1840797e382ba61728d47e corporate/3.0/i586/bind-9.2.3-6.2.C30mdk.i586.rpm
0f1e56f1f3a2689443c04b52d8ce5545 corporate/3.0/i586/bind-devel-9.2.3-6.2.C30mdk.i586.rpm
99bf1f4127e97b8941b597aa5e19aa0a corporate/3.0/i586/bind-utils-9.2.3-6.2.C30mdk.i586.rpm
2b49bd9c7edf8bd81b297260b54de32d corporate/3.0/SRPMS/bind-9.2.3-6.2.C30mdk.src.rpm

Corporate 3.0/X86_64:

e74bea44aee406d11c87227584790c26 corporate/3.0/x86_64/bind-9.2.3-6.2.C30mdk.x86_64.rpm
b108edf227b55f3af3ab55b48c23a62a corporate/3.0/x86_64/bind-devel-9.2.3-6.2.C30mdk.x86_64.rpm
ba548cbba992f479ad40ecf0808f36cb corporate/3.0/x86_64/bind-utils-9.2.3-6.2.C30mdk.x86_64.rpm
2b49bd9c7edf8bd81b297260b54de32d corporate/3.0/SRPMS/bind-9.2.3-6.2.C30mdk.src.rpm

Corporate 4.0:

8bfc97510d4f07568d64c9b9872b4bba corporate/4.0/i586/bind-9.3.2-7.1.20060mlcs4.i586.rpm
dda709703f8bf05f1ff59ae6132a81a7 corporate/4.0/i586/bind-devel-9.3.2-7.1.20060mlcs4.i586.rpm
daf59d23abaaaf62c990d2fa1155688c corporate/4.0/i586/bind-utils-9.3.2-7.1.20060mlcs4.i586.rpm
ccfd1d4d79b168ab5f7998e51c305a26 corporate/4.0/SRPMS/bind-9.3.2-7.1.20060mlcs4.src.rpm

Corporate 4.0/X86_64:

3d1bbe1e7d4f2de6e546996e181a16b0 corporate/4.0/x86_64/bind-9.3.2-7.1.20060mlcs4.x86_64.rpm
c1b8467d62623ef5daf35a696ab2389e corporate/4.0/x86_64/bind-devel-9.3.2-7.1.20060mlcs4.x86_64.rpm
83cf57110f107c450aaac5931ee52ecb corporate/4.0/x86_64/bind-utils-9.3.2-7.1.20060mlcs4.x86_64.rpm
ccfd1d4d79b168ab5f7998e51c305a26 corporate/4.0/SRPMS/bind-9.3.2-7.1.20060mlcs4.src.rpm

Multi Network Firewall 2.0:

[MDKSA-2006:207] – Updated bind packages fixes RSA signature verification vulnerability

```
abd228e7f0b762ae8c11c8ecd90200c2 mnf/2.0/i586/bind-9.2.3-6.2.M20mdk.i586.rpm
dd7b0785e31880a09d10957695c0552d mnf/2.0/i586/bind-devel-9.2.3-6.2.M20mdk.i586.rpm
0a2052e5f263b8b8d94111a581928c57 mnf/2.0/i586/bind-utils-9.2.3-6.2.M20mdk.i586.rpm
eff2c78779b4285783ffea14e6e33c31 mnf/2.0/SRPMS/bind-9.2.3-6.2.M20mdk.src.rpm
```

To upgrade automatically use MandrivaUpdate or urpmi. The verification of md5 checksums and GPG signatures is performed automatically for you.

All packages are signed by Mandriva for security. You can obtain the GPG public key of the Mandriva Security Team by executing:

```
gpg --recv-keys --keyserver pgp.mit.edu 0x22458A98
```

You can view other update advisories for Mandriva Linux at:

<http://www.mandriva.com/security/advisories>

If you want to report vulnerabilities, please contact

security_(at)_mandriva.com

```
Type Bits/KeyID Date User ID
pub 1024D/22458A98 2000-07-10 Mandriva Security Team
<security*mandriva.com>
```

```
-----BEGIN PGP SIGNATURE-----
```

```
Version: GnuPG v1.4.2.2 (GNU/Linux)
```

```
iD8DBQFFWlnDmqjQ0CJFipgRAvI+AKCd5q51CkdHf1UnUJ4imb9Fzl5mZQCfaW5Z
6faoicEmIFqGW4QuEVlhCbU=
=bI0u
```

```
-----END PGP SIGNATURE-----
```