

## **[Full-disclosure] MDKSA-2005:130 – Updated apache packages fix vulnerabilities**

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0090.html>

---

**From:** Mandriva Security Team ([security\\_at\\_mandriva.com](mailto:security_at_mandriva.com))

**Date:** 08/03/05

To: [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)

Date: Wed, 03 Aug 2005 15:57:46 -0600

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

Hash: SHA1

---

### Mandriva Linux Security Update Advisory

---

Package name: apache

Advisory ID: MDKSA-2005:130

Date: August 3rd, 2005

Affected versions: 10.0, 10.1, 10.2, Corporate 3.0,  
Corporate Server 2.1

---

#### Problem Description:

Watchfire reported a flaw that occurred when using the Apache server as a HTTP proxy. A remote attacker could send an HTTP request with both a "Transfer-Encoding: chunked" header and a "Content-Length" header which would cause Apache to incorrectly handle and forward the body of the request in a way that the receiving server processed it as a separate HTTP request. This could be used to allow the bypass of web application firewall protection or lead to cross-site scripting (XSS) attacks (CAN-2005-2088).

The updated packages have been patched to prevent these issues.

---

#### References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2088>

---

## Full-Disclosure: [Full-disclosure] MDKSA-2005:130 – Updated apache packages fix vulnerabilities

### Updated Packages:

#### Mandrakelinux 10.0:

7b647c45b60004470689faf9a461be6c 10.0/RPMS/apache-1.3.29-1.4.100mdk.i586.rpm  
8b185dee42649dd3a56d5cffdd47f31c 10.0/RPMS/apache-devel-1.3.29-1.4.100mdk.i586.rpm  
991592ab1cb3accd8456f748d8dd1d32 10.0/RPMS/apache-modules-1.3.29-1.4.100mdk.i586.rpm  
a8bc7aee751c8a84584fbcc45d24e5d1 10.0/RPMS/apache-source-1.3.29-1.4.100mdk.i586.rpm  
7dde17d7931fcb2c24fdae964c7d2e1 10.0/SRPMS/apache-1.3.29-1.4.100mdk.src.rpm

#### Mandrakelinux 10.0/AMD64:

38a8d4da07d15367f3b6a47507edd4ef amd64/10.0/RPMS/apache-1.3.29-1.4.100mdk.amd64.rpm  
fdb2f8fe48ac0f99dd7b06a77d6df5eb amd64/10.0/RPMS/apache-devel-1.3.29-1.4.100mdk.amd64.rpm  
ac6018c0c08d7c2e77ae7df8744f5cf0 amd64/10.0/RPMS/apache-modules-1.3.29-1.4.100mdk.amd64.rpm  
0cc565a8b52aa6a6a33041a1a33b535 amd64/10.0/RPMS/apache-source-1.3.29-1.4.100mdk.amd64.rpm  
7dde17d7931fcb2c24fdae964c7d2e1 amd64/10.0/SRPMS/apache-1.3.29-1.4.100mdk.src.rpm

#### Mandrakelinux 10.1:

37fd0fb92592efe5a3fe5d5fa89b0c8c 10.1/RPMS/apache-1.3.31-7.2.101mdk.i586.rpm  
3fcc7e95d9def7cb64aeb6d702563498 10.1/RPMS/apache-devel-1.3.31-7.2.101mdk.i586.rpm  
47a376032b85aebc5370bebbac51e38 10.1/RPMS/apache-modules-1.3.31-7.2.101mdk.i586.rpm  
cd6757a1cc0270243fbc63c10508da0b 10.1/RPMS/apache-source-1.3.31-7.2.101mdk.i586.rpm  
99461fdd6a1955961867fa888cc68d8f 10.1/SRPMS/apache-1.3.31-7.2.101mdk.src.rpm

#### Mandrakelinux 10.1/X86\_64:

ac16e81572c092fe5d6448df9442ca8e x86\_64/10.1/RPMS/apache-1.3.31-7.2.101mdk.x86\_64.rpm  
28de6be2c20737d3819a787e310b2707 x86\_64/10.1/RPMS/apache-devel-1.3.31-7.2.101mdk.x86\_64.rpm  
c02b7724a815cfd4cd8e49a1fb016620  
x86\_64/10.1/RPMS/apache-modules-1.3.31-7.2.101mdk.x86\_64.rpm  
8dca2b8497dd582eb732a23933e43a0f x86\_64/10.1/RPMS/apache-source-1.3.31-7.2.101mdk.x86\_64.rpm  
99461fdd6a1955961867fa888cc68d8f x86\_64/10.1/SRPMS/apache-1.3.31-7.2.101mdk.src.rpm

#### Mandrakelinux 10.2:

72a644da1a2b6ca9b108f169f0dcb683 10.2/RPMS/apache-1.3.33-6.1.102mdk.i586.rpm  
9b715d3b8013f3c475ccd2225a70989a 10.2/RPMS/apache-devel-1.3.33-6.1.102mdk.i586.rpm  
9eaa3fa994130d1de447cab50db7d66f 10.2/RPMS/apache-modules-1.3.33-6.1.102mdk.i586.rpm  
3a2908d244f78eb80f529f843ce5c1ac 10.2/RPMS/apache-source-1.3.33-6.1.102mdk.i586.rpm  
4711227c7c38a014663194c198913907 10.2/SRPMS/apache-1.3.33-6.1.102mdk.src.rpm

#### Mandrakelinux 10.2/X86\_64:

d8d495e7b7fc8aa9c1fb15614ae04e34 x86\_64/10.2/RPMS/apache-1.3.33-6.1.102mdk.x86\_64.rpm  
830b2e4bf1b3f9a390c8e7a7846b1353 x86\_64/10.2/RPMS/apache-devel-1.3.33-6.1.102mdk.x86\_64.rpm  
a8b1adc69eaf5dc2b83bf49e84935a81 x86\_64/10.2/RPMS/apache-modules-1.3.33-6.1.102mdk.x86\_64.rpm  
38bd01fe2513c2c10499689d6fe4f1b1 x86\_64/10.2/RPMS/apache-source-1.3.33-6.1.102mdk.x86\_64.rpm  
4711227c7c38a014663194c198913907 x86\_64/10.2/SRPMS/apache-1.3.33-6.1.102mdk.src.rpm

#### Corporate Server 2.1:

9ce162ffa4d94c527ab84e668ae17a78 corporate/2.1/RPMS/apache-1.3.26-7.4.C21mdk.i586.rpm  
4bdd4119a520be80ddd577c0f45acca corporate/2.1/RPMS/apache-common-1.3.26-7.4.C21mdk.i586.rpm  
132604f1487d76a5f5d7ace3ee10c040 corporate/2.1/RPMS/apache-devel-1.3.26-7.4.C21mdk.i586.rpm  
920f9e8aa639db5e55224db2a75e908d corporate/2.1/RPMS/apache-manual-1.3.26-7.4.C21mdk.i586.rpm  
fe919175f6898834f3372f20d76f55df corporate/2.1/RPMS/apache-modules-1.3.26-7.4.C21mdk.i586.rpm

Full-Disclosure: [Full-disclosure] MDKSA-2005:130 – Updated apache packages fix vulnerabilities

64cf8b3d566d5010da1273f1ceeb9416 corporate/2.1/RPMS/apache-source-1.3.26-7.4.C21mdk.i586.rpm  
9a7d8ecb5a9530d17347c5490fe5df87 corporate/2.1/SRPMS/apache-1.3.26-7.4.C21mdk.src.rpm

Corporate Server 2.1/X86\_64:

0dffe139277b76e135e535b4bd4fa79a x86\_64/corporate/2.1/RPMS/apache-1.3.26-7.4.C21mdk.x86\_64.rpm  
8226b7fd08c890401944c5aa490600d2  
x86\_64/corporate/2.1/RPMS/apache-common-1.3.26-7.4.C21mdk.x86\_64.rpm  
69e8a4f73342352b52bf828b2304af18  
x86\_64/corporate/2.1/RPMS/apache-devel-1.3.26-7.4.C21mdk.x86\_64.rpm  
112bde1b90f4741699c5618894c61f99  
x86\_64/corporate/2.1/RPMS/apache-manual-1.3.26-7.4.C21mdk.x86\_64.rpm  
d732d8e462489a368d3c1b237b29570a  
x86\_64/corporate/2.1/RPMS/apache-modules-1.3.26-7.4.C21mdk.x86\_64.rpm  
b40b4e4b81a090015754136d8eeb2e58  
x86\_64/corporate/2.1/RPMS/apache-source-1.3.26-7.4.C21mdk.x86\_64.rpm  
9a7d8ecb5a9530d17347c5490fe5df87 x86\_64/corporate/2.1/SRPMS/apache-1.3.26-7.4.C21mdk.src.rpm

Corporate 3.0:

9b2d7101aa263e860ea3839260620fe6 corporate/3.0/RPMS/apache-1.3.29-1.4.C30mdk.i586.rpm  
be9d739b634cf93d229ad7b65bbf6c28 corporate/3.0/RPMS/apache-modules-1.3.29-1.4.C30mdk.i586.rpm  
7c9f246c832fec1cf3487e516ff334f4 corporate/3.0/SRPMS/apache-1.3.29-1.4.C30mdk.src.rpm

Corporate 3.0/X86\_64:

58bb5e99baa148f0bedf1d8982b3301f x86\_64/corporate/3.0/RPMS/apache-1.3.29-1.4.C30mdk.x86\_64.rpm  
b7de432d1647f4ffe0661e9a921251dd  
x86\_64/corporate/3.0/RPMS/apache-modules-1.3.29-1.4.C30mdk.x86\_64.rpm  
7c9f246c832fec1cf3487e516ff334f4 x86\_64/corporate/3.0/SRPMS/apache-1.3.29-1.4.C30mdk.src.rpm

---

To upgrade automatically use MandrakeUpdate 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>
```

Full-Disclosure: [Full-disclosure] MDKSA-2005:130 – Updated apache packages fix vulnerabilities

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

Version: GnuPG v1.2.4 (GNU/Linux)

iD8DBQFC8T3amqjQ0CJFipgRAhcRAJ9SkX4ucOM7W6WZdSVDqvSNPfvkIwCg9KVb  
kkzYIeE8rAfKpPdxKGbbKVY=  
=fAs6

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

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>