

[MDKSA-2006:133] – Updated apache packages fix mod_rewrite vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-07/msg00529.html>

- *From:* security@xxxxxxxxxxxxx
 - *Date:* Fri, 28 Jul 2006 12:33:00 -0600
-

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

Hash: SHA1

Mandriva Linux Security Advisory MDKSA-2006:133
<http://www.mandriva.com/security/>

Package : apache
Date : July 28, 2006
Affected: 2006.0, Corporate 3.0, Multi Network Firewall 2.0

Problem Description:

Mark Dowd, of McAfee Avert Labs, discovered a potential remotely exploitable off-by-one flaw in Apache's mod_rewrite ldap scheme handling.

In order for this to be exploitable, a number of conditions need to be met including a) running a vulnerable version of Apache (1.3.28+, 2.0.46+, or 2.2.0+), b) enabling mod_rewrite, c) having a rewrite rule that the remote user can influence the beginning of, and d) a particular stack frame layout.

By default, RewriteEngine is not enabled in Mandriva Linux Apache packages, and no RewriteRules are defined.

Updated packages have been patched to correct this issue.

References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3747>

[MDKSA-2006:133] – Updated apache packages fix mod_rewrite vulnerability

Updated Packages:

Mandriva Linux 2006.0:

ebae509678a2c96c28a73630b0c30f23 2006.0/RPMS/apache-base-2.0.54-13.3.20060mdk.i586.rpm
ae7f7ab76fc982e61acb61eda6799299 2006.0/RPMS/apache-devel-2.0.54-13.3.20060mdk.i586.rpm
1c5a8110c41c4c35bdc73e6c9b58ba9a 2006.0/RPMS/apache-mod_cache-2.0.54-13.3.20060mdk.i586.rpm
4fcc04bd44e4000f6550e91b79d3c0ca 2006.0/RPMS/apache-mod_dav-2.0.54-13.3.20060mdk.i586.rpm
76022b54360cfb38fca648d8120b8556 2006.0/RPMS/apache-mod_deflate-2.0.54-13.3.20060mdk.i586.rpm
1066b0d30d2e39515fef3bb54b5bce5b
2006.0/RPMS/apache-mod_disk_cache-2.0.54-13.3.20060mdk.i586.rpm
dde5b8b2072610fb00c734a2e1e9c22a
2006.0/RPMS/apache-mod_file_cache-2.0.54-13.3.20060mdk.i586.rpm
253da3436b3babcb3abb3d1ff7af7 2006.0/RPMS/apache-mod_ldap-2.0.54-13.3.20060mdk.i586.rpm
f0243852a659fef7c03de0c52ccde06
2006.0/RPMS/apache-mod_mem_cache-2.0.54-13.3.20060mdk.i586.rpm
58949e068479c1f93505e74cba4cdeaa 2006.0/RPMS/apache-mod_proxy-2.0.54-13.3.20060mdk.i586.rpm
27d44a61a8dab8c663977e84e60be6c7 2006.0/RPMS/apache-modules-2.0.54-13.3.20060mdk.i586.rpm
f579d113efcc894ee37d5a46b30ff0a6 2006.0/RPMS/apache-mod_userdir-2.0.54-13.3.20060mdk.i586.rpm
f4c30b2c8094d37e0298d491b7d12bba
2006.0/RPMS/apache-mpm-peruser-2.0.54-13.3.20060mdk.i586.rpm
8371dd810a4e1062d3e58beaed76aac
2006.0/RPMS/apache-mpm-prefork-2.0.54-13.3.20060mdk.i586.rpm
60414cc8da66fb5aef97a1fc2dc84527 2006.0/RPMS/apache-mpm-worker-2.0.54-13.3.20060mdk.i586.rpm
877e93cc1f5e623dc4e41a61242f986c 2006.0/RPMS/apache-source-2.0.54-13.3.20060mdk.i586.rpm
0a5859b475b8cb95ff24315da7bafba4 2006.0/SRPMS/apache-2.0.54-13.3.20060mdk.src.rpm

Mandriva Linux 2006.0/X86_64:

ec96c0234417cf8ab9ad4291f43afcd2
x86_64/2006.0/RPMS/apache-base-2.0.54-13.3.20060mdk.x86_64.rpm
c5d0a609cb8d301f0bde876b57e03043
x86_64/2006.0/RPMS/apache-devel-2.0.54-13.3.20060mdk.x86_64.rpm
e9b4613c323e744a5c92e363f088d310
x86_64/2006.0/RPMS/apache-mod_cache-2.0.54-13.3.20060mdk.x86_64.rpm
fba9d1c2ef3bf9598155441cfd396a5c
x86_64/2006.0/RPMS/apache-mod_dav-2.0.54-13.3.20060mdk.x86_64.rpm
75b2ca971f394d2d3711554adb15ffa2
x86_64/2006.0/RPMS/apache-mod_deflate-2.0.54-13.3.20060mdk.x86_64.rpm
fa572adae5767f3151ae48789a9fae00
x86_64/2006.0/RPMS/apache-mod_disk_cache-2.0.54-13.3.20060mdk.x86_64.rpm
aab5e0e796252e752393be0383e37322
x86_64/2006.0/RPMS/apache-mod_file_cache-2.0.54-13.3.20060mdk.x86_64.rpm
e413ad22fa7b802fcb84931d7634bfe2
x86_64/2006.0/RPMS/apache-mod_ldap-2.0.54-13.3.20060mdk.x86_64.rpm
1a9ca26d7b699bef7c39c3bfd8c8f469
x86_64/2006.0/RPMS/apache-mod_mem_cache-2.0.54-13.3.20060mdk.x86_64.rpm
726edc13662c0642f0e09fa800ee1294
x86_64/2006.0/RPMS/apache-mod_proxy-2.0.54-13.3.20060mdk.x86_64.rpm
3236c11431b1ac898850fecc22b14136
x86_64/2006.0/RPMS/apache-modules-2.0.54-13.3.20060mdk.x86_64.rpm
d5e066bed00e53dff692abf34a9870f1
x86_64/2006.0/RPMS/apache-mod_userdir-2.0.54-13.3.20060mdk.x86_64.rpm

[MDKSA-2006:133] – Updated apache packages fix mod_rewrite vulnerability

2b15cdeed5590d6510f9889337680375
x86_64/2006.0/RPMS/apache-mpm-peruser-2.0.54-13.3.20060mdk.x86_64.rpm
0fc37bbfd509933b68460dca2c33b1ac
x86_64/2006.0/RPMS/apache-mpm-prefork-2.0.54-13.3.20060mdk.x86_64.rpm
f6ba45f856a7b0ae79ea3bac4b5adfc0
x86_64/2006.0/RPMS/apache-mpm-worker-2.0.54-13.3.20060mdk.x86_64.rpm
ec72f9d159ea8ea0b8b0cafd5946f49c
x86_64/2006.0/RPMS/apache-source-2.0.54-13.3.20060mdk.x86_64.rpm
0a5859b475b8cb95ff24315da7bafba4 x86_64/2006.0/SRPMS/apache-2.0.54-13.3.20060mdk.src.rpm

Corporate 3.0:

566a5494c3a14c5e176a750a7997869e corporate/3.0/RPMS/apache-1.3.29-1.5.C30mdk.i586.rpm
cebb813717c0f08571fee33e07f42bc1 corporate/3.0/RPMS/apache2-2.0.48-6.13.C30mdk.i586.rpm
3fa46c76c1a5a263317b4799848d7e6c
corporate/3.0/RPMS/apache2-common-2.0.48-6.13.C30mdk.i586.rpm
527c568c24872c6f964ca6c9e36ec118 corporate/3.0/RPMS/apache2-devel-2.0.48-6.13.C30mdk.i586.rpm
115bdb5fd40b900f0ef0d2473f59948a corporate/3.0/RPMS/apache2-manual-2.0.48-6.13.C30mdk.i586.rpm
a238d2e3001cc92838c6deb6d3572f38
corporate/3.0/RPMS/apache2-mod_cache-2.0.48-6.13.C30mdk.i586.rpm
fce77bec697fba16111c21abae012e45
corporate/3.0/RPMS/apache2-mod_dav-2.0.48-6.13.C30mdk.i586.rpm
19df98830307120d322139909c72521c
corporate/3.0/RPMS/apache2-mod_deflate-2.0.48-6.13.C30mdk.i586.rpm
bdf826b0d24df2782efe7a533e2bef0c
corporate/3.0/RPMS/apache2-mod_disk_cache-2.0.48-6.13.C30mdk.i586.rpm
7d0135ffdf47f14bc1f247429cb817e4
corporate/3.0/RPMS/apache2-mod_file_cache-2.0.48-6.13.C30mdk.i586.rpm
1dfd528875f1a013ecc649f3496a9319
corporate/3.0/RPMS/apache2-mod_ldap-2.0.48-6.13.C30mdk.i586.rpm
792af80955c5bbf0db335d53b1fca13c
corporate/3.0/RPMS/apache2-mod_mem_cache-2.0.48-6.13.C30mdk.i586.rpm
fbcdf89e26e8f55936eefd836e48
corporate/3.0/RPMS/apache2-mod_proxy-2.0.48-6.13.C30mdk.i586.rpm
c85871f0a60bbf10f9af9805e97dba34 corporate/3.0/RPMS/apache2-mod_ssl-2.0.48-6.13.C30mdk.i586.rpm
d710c931c7e7005cfe77ddc0ef584947 corporate/3.0/RPMS/apache2-modules-2.0.48-6.13.C30mdk.i586.rpm
5a07d3b609ce4613755f031bb4025819 corporate/3.0/RPMS/apache2-source-2.0.48-6.13.C30mdk.i586.rpm
c17733e580d25fa041886e9cd35b9322 corporate/3.0/RPMS/apache-devel-1.3.29-1.5.C30mdk.i586.rpm
9b826a4fa35a3235ed3aedfd0b44609 corporate/3.0/RPMS/apache-modules-1.3.29-1.5.C30mdk.i586.rpm
9d9a2747b98ec88394a4a59390b7a7c4 corporate/3.0/RPMS/apache-source-1.3.29-1.5.C30mdk.i586.rpm
9113740cc7abbbec586137bb7018c270 corporate/3.0/RPMS/libapr0-2.0.48-6.13.C30mdk.i586.rpm
3f6688dd5ba8982ca9d1277b78ac119b corporate/3.0/SRPMS/apache-1.3.29-1.5.C30mdk.src.rpm
d6d2282793e20880c3975ea80b907674 corporate/3.0/SRPMS/apache2-2.0.48-6.13.C30mdk.src.rpm

Corporate 3.0/X86_64:

617acd26211661d3b93d34b415b13eb0
x86_64/corporate/3.0/RPMS/apache-1.3.29-1.5.C30mdk.x86_64.rpm
b38b1f3efbc0795b433a994abba9a8f7
x86_64/corporate/3.0/RPMS/apache2-2.0.48-6.13.C30mdk.x86_64.rpm
2adc7e3a0de0c9cec65f6a125bade13a
x86_64/corporate/3.0/RPMS/apache2-common-2.0.48-6.13.C30mdk.x86_64.rpm
cad9c4879077026df3e1db8dd30bf1c9

[MDKSA-2006:133] – Updated apache packages fix mod_rewrite vulnerability

x86_64/corporate/3.0/RPMS/apache2-devel-2.0.48-6.13.C30mdk.x86_64.rpm
31b72d855febf7bd27f755a5252a225f
x86_64/corporate/3.0/RPMS/apache2-manual-2.0.48-6.13.C30mdk.x86_64.rpm
2301e27667996ee9dd9f7c54bbbf7b38
x86_64/corporate/3.0/RPMS/apache2-mod_cache-2.0.48-6.13.C30mdk.x86_64.rpm
0b26b6262eb76e6cae28096bccbe525c
x86_64/corporate/3.0/RPMS/apache2-mod_dav-2.0.48-6.13.C30mdk.x86_64.rpm
cd00509b19c01e89743506945d79b741
x86_64/corporate/3.0/RPMS/apache2-mod_deflate-2.0.48-6.13.C30mdk.x86_64.rpm
40172eb4e8f02bf5687c91185cdc823c
x86_64/corporate/3.0/RPMS/apache2-mod_disk_cache-2.0.48-6.13.C30mdk.x86_64.rpm
07d0bbfdb795c4303a1c9a840f428154
x86_64/corporate/3.0/RPMS/apache2-mod_file_cache-2.0.48-6.13.C30mdk.x86_64.rpm
8798865d801abf9ffc062f29f51ae34b
x86_64/corporate/3.0/RPMS/apache2-mod_ldap-2.0.48-6.13.C30mdk.x86_64.rpm
025d53b2271429d014017a9af763dc8a
x86_64/corporate/3.0/RPMS/apache2-mod_mem_cache-2.0.48-6.13.C30mdk.x86_64.rpm
f9f9c0f581ffe083f9ce3d8506e054a8
x86_64/corporate/3.0/RPMS/apache2-mod_proxy-2.0.48-6.13.C30mdk.x86_64.rpm
a01c2c6b91bb6c237f40b1bbf8fda5df
x86_64/corporate/3.0/RPMS/apache2-mod_ssl-2.0.48-6.13.C30mdk.x86_64.rpm
79b6ee6c17e04ec63fda6f81bc5a5501
x86_64/corporate/3.0/RPMS/apache2-modules-2.0.48-6.13.C30mdk.x86_64.rpm
63fa68ca230b4f1e704912ed1ae28522
x86_64/corporate/3.0/RPMS/apache2-source-2.0.48-6.13.C30mdk.x86_64.rpm
4cc0f5c8c21edb50cbb2e3170053fea3
x86_64/corporate/3.0/RPMS/apache-devel-1.3.29-1.5.C30mdk.x86_64.rpm
ea1ccb27856c858ed0093825b0d9157c
x86_64/corporate/3.0/RPMS/apache-modules-1.3.29-1.5.C30mdk.x86_64.rpm
3e1ef8a32185108b14b392597d652634
x86_64/corporate/3.0/RPMS/apache-source-1.3.29-1.5.C30mdk.x86_64.rpm
365d9820028c26f3b9de6bd75056c383
x86_64/corporate/3.0/RPMS/lib64apr0-2.0.48-6.13.C30mdk.x86_64.rpm
3f6688dd5ba8982ca9d1277b78ac119b x86_64/corporate/3.0/SRPMS/apache-1.3.29-1.5.C30mdk.src.rpm
d6d2282793e20880c3975ea80b907674 x86_64/corporate/3.0/SRPMS/apache2-2.0.48-6.13.C30mdk.src.rpm

Multi Network Firewall 2.0:

bc009b09567626e607218d70f260cafa mnf/2.0/RPMS/apache2-2.0.48-6.13.M20mdk.i586.rpm
f06196a72fbbb40f897f701f63defe74 mnf/2.0/RPMS/apache2-common-2.0.48-6.13.M20mdk.i586.rpm
49fed15cff4348b2bd162a2b612a7c09 mnf/2.0/RPMS/apache2-devel-2.0.48-6.13.M20mdk.i586.rpm
e0848b25ece016c968d1f03900d05b25 mnf/2.0/RPMS/apache2-manual-2.0.48-6.13.M20mdk.i586.rpm
d2adbf4cb660b2e8b8414b4b12995ee9 mnf/2.0/RPMS/apache2-mod_cache-2.0.48-6.13.M20mdk.i586.rpm
500fcb76763df7d1999c9c30aec6f339 mnf/2.0/RPMS/apache2-mod_dav-2.0.48-6.13.M20mdk.i586.rpm
8899cba4166e9aa426b71a16ebce4399 mnf/2.0/RPMS/apache2-mod_deflate-2.0.48-6.13.M20mdk.i586.rpm
9d118e749e50e7945d8f4f304c822433
mnf/2.0/RPMS/apache2-mod_disk_cache-2.0.48-6.13.M20mdk.i586.rpm
a2b22dfea4eee15fbd47bad5b625b4c3
mnf/2.0/RPMS/apache2-mod_file_cache-2.0.48-6.13.M20mdk.i586.rpm
6e88df28f77bf2bbc8c665d610a7391 mnf/2.0/RPMS/apache2-mod_ldap-2.0.48-6.13.M20mdk.i586.rpm
827ef114c1801e4139571b0f87115a78
mnf/2.0/RPMS/apache2-mod_mem_cache-2.0.48-6.13.M20mdk.i586.rpm

[MDKSA-2006:133] – Updated apache packages fix mod_rewrite vulnerability

d10842201c502da141df43d21c7840b3 mnf/2.0/RPMS/apache2-mod_proxy-2.0.48-6.13.M20mdk.i586.rpm
17be96783ed2c46212aa18014c75c00e mnf/2.0/RPMS/apache2-mod_ssl-2.0.48-6.13.M20mdk.i586.rpm
5abc11514ddb9c5235a3a409bc98860a mnf/2.0/RPMS/apache2-modules-2.0.48-6.13.M20mdk.i586.rpm
c15499d0be66da28b0030ce0ba458399 mnf/2.0/RPMS/apache2-source-2.0.48-6.13.M20mdk.i586.rpm
ecc2534b32ea7b9dcc08b0bc27ad2f79 mnf/2.0/RPMS/libapr0-2.0.48-6.13.M20mdk.i586.rpm
52f87a940c2058d8d5da18bc53f78e25 mnf/2.0/SRPMS/apache2-2.0.48-6.13.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)
```

```
iD8DBQFEyiuBmqjQ0CJFipgRAjfyAJ9gY11291imG1EwXNjOIResx6RgagCfR2Wz  
mPbs0TLuI3ZpwgUWGqCGhkU=  
=H0Ni  
-----END PGP SIGNATURE-----
```