

TSLSA-2005-0038 – multi

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-08/0008.html>

From: Trustix Security Advisor (*tsl_at_trustix.org*)

Date: 08/01/05

Date: Mon, 1 Aug 2005 15:12:50 +0200

To: bugtraq@securityfocus.com

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

Hash: SHA1

Trustix Secure Linux Security Advisory #2005-0038

Package name: mysql, fetchmail, zlib, perl, apache
 netpbm, vim, nss_ldap

Summary: Multiple vulnerabilities

Date: 2005-07-29

Affected versions: Trustix Secure Linux 2.2

 Trustix Secure Linux 3.0

 Trustix Operating System – Enterprise Server 2

Package Description:

apache

Apache is a full featured web server that is freely available, and also happens to be the most widely used.

fetchmail

Fetchmail is a remote mail retrieval and forwarding utility intended for use over on-demand TCP/IP links, like SLIP or PPP connections. Fetchmail supports every remote-mail protocol currently in use on the Internet (POP2, POP3, RPOP, APOP, KPOP, all IMAPs, ESMTP ETRN, IPv6, and IPSEC) for retrieval. Then Fetchmail forwards the mail through SMTP so you can read it through your favorite mail client.

mysql

MySQL is a true multi-user, multi-threaded SQL (Structured Query Language) database server. MySQL is a client/server implementation that consists of a server daemon (mysqld) and many different client programs/libraries.

netpbm

The netpbm package contains a library of functions which support

programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps) and others.

nss_ldap

This package includes a LDAP access client: nss_ldap. Nss_ldap is a set of C library extensions which allows X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services and shadow passwords (instead of or in addition to using flat files or NIS).

perl

Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications (and what it excels at) are probably system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts.

vim

VIM (VIual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting and more.

zlib

The zlib compression library provides in-memory compression and decompression functions, including integrity checks of the uncompressed data. This version of the library supports only one compression method (deflation), but other algorithms may be added later, which will have the same stream interface. The zlib library is used by many different system programs.

Problem Description:

apache

- Security Fix:
- Watchfire reported a flaw that occurred when using the Apache server as an HTTP proxy. A remote attacker could send an HTTP request with both a "Transfer-Encoding: chunked" header and a "Content-Length" header. This caused Apache to incorrectly handle and forward the body of the request in a way that the receiving server processes it as a separate HTTP request. This could allow the bypass of Web application firewall protection or lead to cross-site scripting (XSS) attacks.
- Marc Stern reported an off-by-one overflow in the mod_ssl CRL verification callback. In order to exploit this issue the Apache server would need to be configured to use a malicious certificate revocation list (CRL).

The Common Vulnerabilities and Exposures project (cve.mitre.org) assigned the name CAN-2005-2088 and CAN-2005-1268 to this issue.

fetchmail

- New Upstream
- Security Fix: Remote code injection vulnerability in fetchmail
- The POP3 code that deals with UIDs (from the UIDL) reads the responses returned by the POP3 server into fixed-size buffers allocated on the stack, without limiting the input length to the buffer size. A compromised or malicious POP3 server can thus overrun fetchmail's stack. This affects POP3 and all of its variants, for instance but not limited to APOP.

mysql

- New Upstream
- Security Fix: MySQL uses a vulnerable version of the zlib library which can be exploited by malicious users to cause a DoS (Denial of Service), or potentially by malicious people to execute arbitrary code. It is possible for malicious users to crash the server in various ways.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-2096.

netpbm

- Security Fix: Max Vozeler has reported a vulnerability in netpbm, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to pstopnm not using the "-dSAFER" option when calling GhostScript to convert a PostScript file into a PBM, PGM, or PNM file. This allows a malicious PostScript file to execute arbitrary commands on a vulnerable system.

nss_ldap

- Security Fix: Plain text authentication leak.
- nss_ldap when used with OpenLDAP and connecting to a slave using TLS, does not use TLS for the subsequent connection if the client is referred to a master, which may cause a password to be sent in cleartext and allows remote attackers to sniff the password.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-2069 to this issue.

perl

- Security Fix: Race condition in the rmtree function in Perl
- Race condition in the rmtree function in the File::Path module sets read/write permissions for the world, which allows local users to delete arbitrary files and directories, and possibly read files and directories, via a symlink attack.

SecurityFocus Bugtraq: TSLSA-2005-0038 – multi

- Race condition in the rmtree function in File::Path.pm allows local users to create arbitrary setuid binaries in the tree being deleted.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0452 and CAN-2005-0448 to this issue.

vim

- Fix vulnerability in vim, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an error that allows the "glob()" command to be exploited to execute shell commands when the user opens a specially crafted file. Credits to Georgi Guninski.
- Added patches from 048-085

zlib

- Vendor fixes for previous security fixes
- Security Fix: Eliminates potential vulnerability when decoding invalid compressed data
- Security Fix: Eliminates potential vulnerability when decoding specially crafted compressed data
- Bug Fix: Fixes a bug when decompressing dynamic blocks with no distance codes.
- Fixes crc check in gzread() after gzungetc()
- Does not return an error when using gzread() on an empty file

Action:

We recommend that all systems with this package installed be upgraded. Please note that if you do not need the functionality provided by this package, you may want to remove it from your system.

Location:

All Trustix Secure Linux updates are available from
<URI:<http://http.trustix.org/pub/trustix/updates/>>
<URI:<ftp://ftp.trustix.org/pub/trustix/updates/>>

About Trustix Secure Linux:

Trustix Secure Linux is a small Linux distribution for servers. With focus on security and stability, the system is painlessly kept safe and up to date from day one using swup, the automated software updater.

Automatic updates:

Users of the SWUP tool can enjoy having updates automatically installed using 'swup --upgrade'.

Questions?

Check out our mailing lists:
<URI:<http://www.trustix.org/support/>>

Verification:

This advisory along with all Trustix packages are signed with the

SecurityFocus Bugtraq: TLSA-2005-0038 – multi

TSL sign key.

This key is available from:

<URI:<http://www.trustix.org/TSL-SIGN-KEY>>

The advisory itself is available from the errata pages at

<URI:<http://www.trustix.org/errata/trustix-2.2/>> and

<URI:<http://www.trustix.org/errata/trustix-3.0/>>

or directly at

<URI:<http://www.trustix.org/errata/2005/0038/>>

MD5sums of the packages:

8619bcaadf658ab336a119bf8526a2c9 3.0/rpms/apache-2.0.54-11tr.i586.rpm
db50afd388b73797a3ebba39422cdba2 3.0/rpms/apache-dbm-2.0.54-11tr.i586.rpm
6562d0e45bd50f9a363643305b8f0d08 3.0/rpms/apache-devel-2.0.54-11tr.i586.rpm
2a980b79b55ec9a8a287526c023cba79 3.0/rpms/apache-html-2.0.54-11tr.i586.rpm
4ebd1134560782f0a9e806a9399d87a4 3.0/rpms/apache-manual-2.0.54-11tr.i586.rpm
c44ad0246640ca1726c13ca7e62efab0 3.0/rpms/fetchmail-6.2.5.2-1tr.i586.rpm
cbd289e2af78a7a7a685e0d2f7692ee5 3.0/rpms/mysql-4.1.13-1tr.i586.rpm
1263ff0cca93ea99f8dbf89832cf5de8 3.0/rpms/mysql-bench-4.1.13-1tr.i586.rpm
f148db613aa4c7bf5f86f651cc92c8b4 3.0/rpms/mysql-client-4.1.13-1tr.i586.rpm
5a7ba110a918b2e93e6da84ec160abcf 3.0/rpms/mysql-devel-4.1.13-1tr.i586.rpm
e36aa7a70f5086166ee3e91f0c4e5b9c 3.0/rpms/mysql-libs-4.1.13-1tr.i586.rpm
920eb153b5956b39b8cb4a6aa3438231 3.0/rpms/mysql-shared-4.1.13-1tr.i586.rpm
022e95582cb13cb1c625e5d969ba7910 3.0/rpms/netpbm-10.27-4tr.i586.rpm
28151fbbad0fec8ceb7f058d9ee214cf 3.0/rpms/netpbm-devel-10.27-4tr.i586.rpm
1c1d6f8dc7694f48a8373fed81498adf 3.0/rpms/netpbm-progs-10.27-4tr.i586.rpm
e84cfc37fb548c15b814ec82addc73dc 3.0/rpms/nss_ldap-238-7tr.i586.rpm
1c6066a828529905658da0a3680e44b3 3.0/rpms/perl-5.8.7-1tr.i586.rpm
ce6db485d76fec1cb419d277fcfe9c99 3.0/rpms/vim-6.3.085-7tr.i586.rpm
375d53b62b14aea4b9ab60251d379d23 3.0/rpms/vim-doc-6.3.085-7tr.i586.rpm
cee37c97ab9bc7cc830dc28351ec6a23 3.0/rpms/vim-syntax-6.3.085-7tr.i586.rpm
955fc8c2e8e88e88b8bae4400cdc5e93 3.0/rpms/vim-tools-6.3.085-7tr.i586.rpm
17a3d77206110f44fadad9e13cd42030 3.0/rpms/zlib-1.2.3-1tr.i586.rpm
b39665868152f813a12389e41274d25c 3.0/rpms/zlib-devel-1.2.3-1tr.i586.rpm

870f2f5dba2e9a44e3f3d70ff49c1102 2.2/rpms/apache-2.0.54-5tr.i586.rpm
f613e5ddc1fbc430faefe642ecb142a2 2.2/rpms/apache-dbm-2.0.54-5tr.i586.rpm
5015b221276ff2a6b97d685cac5a3902 2.2/rpms/apache-devel-2.0.54-5tr.i586.rpm
ad08be046799c539b628a4c1171ac205 2.2/rpms/apache-html-2.0.54-5tr.i586.rpm
379504cdb392aae650b4bf89ff6934ce 2.2/rpms/apache-manual-2.0.54-5tr.i586.rpm
9f72920a251ab3b0724f04baf9917121 2.2/rpms/fetchmail-6.2.5.2-1tr.i586.rpm
4abc0aaa694964c69b5eb881ec092b88 2.2/rpms/mysql-4.1.13-1tr.i586.rpm
f8e33408c7b54484e19a90acd91c1d03 2.2/rpms/mysql-bench-4.1.13-1tr.i586.rpm
5a8af66af1b162888877aa8c106e67d7 2.2/rpms/mysql-client-4.1.13-1tr.i586.rpm
29f5edd82ef59729eba924f343adbaaf 2.2/rpms/mysql-devel-4.1.13-1tr.i586.rpm
efed0622e6466053cff2afce4d79ba2a 2.2/rpms/mysql-libs-4.1.13-1tr.i586.rpm
65a2625c8ab445c647773df59a96f336 2.2/rpms/mysql-shared-4.1.13-1tr.i586.rpm
293688b542ed68db7cac3bdd3ed74bfa 2.2/rpms/netpbm-10.27-3tr.i586.rpm
567c165a6c3005013760d077ba98ae8d 2.2/rpms/netpbm-devel-10.27-3tr.i586.rpm
66aa0b76eaa83947cfbf84b7ab2a250b 2.2/rpms/netpbm-progs-10.27-3tr.i586.rpm

SecurityFocus Bugtraq: TSLSA-2005-0038 – multi

5a3b7ad1a9e69d8fc065c69d999e63b9 2.2/rpms/nss_ldap-220-2tr.i586.rpm
4853b2be6fcc87d4053abe47000f44b1 2.2/rpms/perl-5.8.5-8tr.i586.rpm
80debae9f4834c34f069caa1ea45006e 2.2/rpms/vim-6.3.085-5tr.i586.rpm
07e838e3407db4e10a64bfc3d508675 2.2/rpms/vim-doc-6.3.085-5tr.i586.rpm
983c3a69a1ad719ff329ecfe75d35084 2.2/rpms/vim-syntax-6.3.085-5tr.i586.rpm
ec59b83ab4937ce33fef90e6e4d763df 2.2/rpms/vim-tools-6.3.085-5tr.i586.rpm
63683076676f076bac3885b277d5ff38 2.2/rpms/zlib-1.2.3-1tr.i586.rpm
f89a4946c772f23ca7db98e13a74001d 2.2/rpms/zlib-devel-1.2.3-1tr.i586.rpm

Trustix Security Team

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

Version: GnuPG v1.4.1 (GNU/Linux)

iD8DBQFC7h45i8CEzsK9IksRAuCCA KC00Ewp93+3Bx7k/Vy1h2PszU23NgCdFzY1
E8HUNPKNbewBYpTeqk4Td7E=
=7mrp

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