

# [UNIX] xmysqladmin Insecure Temporary File Creation

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0033.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 06/12/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 12 Jun 2005 11:13:44 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

xmysqladmin Insecure Temporary File Creation

---

## SUMMARY

"xMySQLadmin is a front end to the MySQL database engine. It allows reloads, status check, process control, isamcheck, grant/revoke privileges, creating databases, dropping databases, and creating, altering, and dropping tables."

By symbolically linking a valid file to the name of a temporary file, attackers can cause xmysqladmin to rewrite the content of that file.

## DETAILS

Vulnerable Systems:

\* xmysqladmin version 1.0

xmysqladmin does not validate the existence of a temporary file. By creating a symbolic link to file with the name of the temporary file, it is possible to override the content of the linked file.

Vulnerable code:

Makefile:

## Securiteam: [UNIX] xmysqladmin Insecure Temporary File Creation

BACKUPDIR = /tmp

In createDropDB.c : begin line 94

```
void dropdb_drop(FL_OBJECT *obj, long data)
{
    char *cmd;

    if(!fl_show_question("WARNING!!!\nThis database will be delete.\nDo
you want to continue?", 0))
        return;
    if(!fl_show_question("WARNING!!!\nThis database will be delete.\nAre
you sure?", 0))
        return;

    cmd = (char *) malloc(2048);
    if(!cmd) return;

    sprintf(cmd, "%s %s/%s.tar%s %s%s/*", BACKUP, BACKUPDIR,
g_dropdb_dbfname,
        BACKUPSUFFIX, Setup.datapath, g_dropdb_dbfname);

    fl_show_command_log(FL_TRANSIENT);
    fl_exe_command(cmd, 1);
    free(cmd);

    {
        MYSQL connection;
        if(g_mysql_connect(&connection, Setup.host, Setup.user,
Setup.password))
        {
            if(mysql_drop_db(&connection, g_dropdb_dbfname))
            {
                fl_show_alert(mysql_error(&connection), "", "", 0);
            }
            else
            {
                fl_show_message("The database", g_dropdb_dbfname, "has been
destroyed");
            }

            mysql_close(&connection);
        }
        else
        {
            fl_show_alert("Cannot connect to server", "", "", 0);
        }
    }
}
```

Disclosure Timeline:

Discovered: 2005-05-24

Vendor notified: 2005-05-29

Securiteam: [UNIX] xmysqladmin Insecure Temporary File Creation

Disclosure: 2005-05-29

ADDITIONAL INFORMATION

The information has been provided by <mailto:exploits@zataz.net> ZATAZ Audits.

The original article can be found at:

<<http://www.zataz.net/adviso/xmysqladmin-05292005.txt>>

<http://www.zataz.net/adviso/xmysqladmin-05292005.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.