

# [UNIX] mysqlhotcopy Insecure Temporary File (copy\_index)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0067.html>

---

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

**Date:** 08/18/04

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

Date: 18 Aug 2004 14:23:51 +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>

-----

mysqlhotcopy Insecure Temporary File (copy\_index)

---

## SUMMARY

mysqlhotcopy is "a fast on-line hot-backup utility for local MySQL databases and tables".

A vulnerability in mysqlhotcopy allows local attackers to cause the product to overwrite create a symbolic link in the /tmp/ directory that will be then overwritten by the mysqlhotcopy utility.

## DETAILS

Insecure temporary file vulnerability in the mysqlhotcopy script has been discovered. This insecure temporary file occurs when using the scp (Secure CoPy) method that is part of the mysql-server package. Creating a temporary file whose name is predictable enough to allow overwriting of arbitrary files causes the vulnerability.

Vulnerable code:

Under the function copy\_index, the following code can be seen:

```
my $tmpfile="$opt_tmpdir/mysqlhotcopy$$";
```

## Securiteam: [UNIX] mysqlhotcopy Insecure Temporary File (copy\_index)

This file is then written to by the script.

Patch:

The following is Debian's mysqlhotcopy provided patch:

```
--- mysql-3.23.49.orig/scripts/mysqlhotcopy.sh
+++ mysql-3.23.49/scripts/mysqlhotcopy.sh
@@ -7,6 +7,8 @@
 use File::Path;
 use DBI;
 use Sys::Hostname;
+use File::Copy;
+use File::Temp;

=head1 NAME

@@ -585,7 +587,6 @@
 sub copy_index
 {
   my ($method, $files, $source, $target) = @_ ;
- my $tmpfile="$Sopt_tmpdir/mysqlhotcopy$$";

   print "Copying indices for ".$files." files...\n" unless $opt{quiet};
   foreach my $file (@$files)
@@ -613,21 +614,21 @@
   }
   elsif ($opt{method} eq 'scp')
   {
- my $tmp=$tmpfile;
- open(OUTPUT,">$tmp") || die "Can't create file $tmp: $!\n";
- if (syswrite(OUTPUT,$buff) != length($buff))
+ my ($fh, $tmp)=tempfile('mysqlhotcopy-XXXXXX', DIR => $opt_tmpdir);
+ die "Can't create/open file in $opt_tmpdir\n";
+ if (syswrite($fh,$buff) != length($buff))
     {
       die "Error when writing data to $tmp: $!\n";
     }
- close OUTPUT || die "Error on close of $tmp: $!\n";
- safe_system("scp $tmp $to");
+ close $fh || die "Error on close of $tmp: $!\n";
+ safe_system("$opt{method} $tmp $to");
+ unlink $tmp;
   }
   else
     { die "Can't use unsupported method '$opt{method}'\n";
     }
- unlink "$tmpfile" if ($opt{method} eq 'scp');
}

```

ADDITIONAL INFORMATION

Securiteam: [UNIX] mysqlhotcopy Insecure Temporary File (copy\_index)

The information has been provided by <mailto:jeroen@wolffelaar.nl> Jeroen van Wolffelaar.

=====

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.