

[UNIX] bsdmainutils Local Root Compromise

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0003.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/01/04

To: list@securiteam.com

Date: 1 Sep 2004 14:05:55 +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>

bsdmainutils Local Root Compromise

SUMMARY

<<http://packages.debian.org/unstable/utils/bsdmainutils>> bsdmainutils is "a collection of small programs many people expect to find when they use a BSD-style UNIX system. Included are: banner, ncal, cal, calendar, col, colcrt, colrm, column, from, hexdump, look, lorder, ul and write".

A vulnerability in its calendar program allows local users to gain root privileges by causing the program to include sensitive files in its event notification emails.

DETAILS

Vulnerable Systems:

* bsdmainutils version 6.0.14 and prior

Immune Systems:

* bsdmainutils version 6.0.1 or newer

How calendar works

The calendar program uses event files with this format:

<date><tab><event description>

Securiteam: [UNIX] bsdmainutils Local Root Compromise

This is not all however. Calendar gives users the ability to include other event-files and define variables and macros. To do this, it calls cpp (the C preprocessor) on the main event file and processes the output.

When called with the "-a" option, calendar will processes the event files of all users and send the result by mail.

The bsdmainutils package in Debian uses this feature from: /etc/cron.daily/bsdmainutils. Luckily, it is not enabled by default since you have to comment an "exit 0" line in the cron script to activate it.

The problem:

Calendar does not drop its privileges. In order to be useful when running with the "-a" option, it needs to run as root. By creating an event file as follows, we can get the hashed root password (on June 28th):

```
#define root Jun. 28<tab>cut_here
#include </etc/shadow>
Jun. 28<tab>Birthday of Steven Van Acker
Aug. 19<tab>Birthday of Andrew Griffith
```

(<tab> indicates an actual tab, so char '\t')

Since calendar is running as root, there will be no problem accessing the shadow password file. The result contains the hashed password of root, which can then be cracked.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0793>>
CAN-2004-0793

ADDITIONAL INFORMATION

The information has been provided by <mailto:deepstar@ulyssis.org> Steven Van Acker.

=====

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.