

[UNIX] Inter7 VPopmail DB Password Problem

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0032.html>

From: support@securiteam.com

Date: 09/06/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] Inter7 VPopmail DB Password Problem

Message-Id: <20010906184317.AA2BD138C0@mail.der-keiler.de>

Date: Thu, 6 Sep 2001 20:43:17 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Inter7 VPopmail DB Password Problem

SUMMARY

VPopmail contains the SQL password in one of its binaries. This, combined with bad default permissions to the binary allows users with read permission to the VPopmail binaries to extract the SQL password and gain access to the database.

DETAILS

Vulnerable systems:

VPopmail version 4.10.35 and prior (When using MySQL)

Immune systems:

VPopmail not using MySQL

The passwords to the MySQL server are compiled into libvpopmail.a, which means that it is rather easy to extract them (a short description for FreeBSD 4.3/gcc 2.95.2 is below). Since all the command line utilities link against libvpopmail.a, they all contain the passwords as well. This means that there is absolutely no needs to write some code that will segfault, as all binaries are chmod 755 that means that every user can read their contents, including the passwords.

Securiteam: [UNIX] Inter7 VPopmail DB Password Problem

Principal attack:

On FreeBSD 4.3/gcc 2.95.2 and vpopmail-4.10.35/4.10 (first one is the development snapshot) the username and password are saved in the same line as the error message "could not connect to MySQL". All you have to do now is open the file in a text editor, search for the string and grab the passwords a few bytes earlier. You can connect to the DB server and do whatever you like.

In some versions, this probably involves access to forwards which means that you could be able to spawn an arbitrary executable under the uid vpopmail runs.

Background:

It is widely known that saving DB passwords anywhere on the system causes a big risk that they will be stolen. However, there is no other solution for daemons to work with databases, as it is obviously impossible to run them interactively typing the password every time they are used. There is not any real solution against this for interpreted code, but for binaries, one can at least remove the r bits from the permissions to prevent users stealing the passwords out of the binaries. Note that there may be many other programs out there that suffer of the same problem.

Solution:

```
# chmod 711 ~vpopmail/bin/*
```

```
# chmod 400 ~vpopmail/lib/*
```

(Substitute the second argument with the directory vpopmail is located on your system, if needed). Alternatively, install the latest vpopmail release, where the binaries are installed this way from begin with. Another approach would be to run qmail/vpopmail on a dedicated server without any users despite root but we understand that this is not an option in many environments.

Final comments:

With the increasing dependence on DBMS (not just MySQL) for more and more tools which potentially could do a lot of damage to the system given the DBMS data is altered in a malicious way, it becomes increasingly important that the DBMS is secure.

ADDITIONAL INFORMATION

The information has been provided by <mailto:gabriel_ambuehl@buz.ch>
Gabriel Ambuehl.

=====

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

=====

=====

Securiteam: [UNIX] Inter7 VPopmail DB Password Problem

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.

- ***Previous message:*** support@securiteam.com: "[\[UNIX\] ShopPlus Arbitrary Command Execution Vulnerability](#)"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)