

[UNIX] Jailed Processes Can Attach To Other Jail

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0013.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/07/04

To: list@securiteam.com

Date: 7 Mar 2004 12:49:16 +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>

Jailed Processes Can Attach To Other Jail

SUMMARY

The jail(2) system call allows a system administrator to lock up a process and all its descendants inside a closed environment with very limited ability to affect the system outside that environment, even for processes with superuser privileges. It is an extension of, but far more stringent than, the traditional Unix chroot(2) system call.

A vulnerability in the jail_attach(2) system process allows a process with superuser privileges inside a jail to change its root directory to that of a different jail, and thus gain full read and write access to files and directories within the target jail.

DETAILS

The jail_attach(2) system call, which was introduced in FreeBSD 5 before 5.1-RELEASE, allows a non-jailed process to permanently move into an existing jail. A programming error has been found in the jail_attach(2) system call which affects the way that system call verifies the privilege level of the calling process. Instead of failing immediately if the calling process was already jailed, the jail_attach(2) system call would fail only after changing the calling process's root directory.

Securiteam: [UNIX] Jailed Processes Can Attach To Other Jail

Solution:

Do one of the following:

1) Upgrade your vulnerable system to 5.2.1-RELEASE, or to the RELENG_5_2 or RELENG_5_1 security branch dated after the correction date.

2) Patch your present system: The following patch has been verified to apply to FreeBSD 5.1 and 5.2 systems.

Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:03/jail.patch
```

```
# fetch
```

```
ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:03/jail.patch.asc
```

Apply the patch:

```
# cd /usr/src
```

```
# patch < /path/to/patch
```

Recompile your kernel as described in and reboot the system.

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:security-advisories@freebsd.org>> FreeBSD Security Advisories.

=====

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.