

[UNIX] NetBSD Kernel swapctl(2) DoS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0055.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 06/17/04

To: list@securiteam.com

Date: 17 Jun 2004 20:32:36 +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>

NetBSD Kernel swapctl(2) DoS Vulnerability

SUMMARY

There exists a integer handling vulnerability in NetBSD swapctl(2) system call used to manage the server's swap file. It seems that this vulnerability cannot be exploited to gain super-user privileges, but any local attacker can crash the kernel.

DETAILS

Vulnerable Systems:

- * NetBSD version 1.6
- * NetBSD version 1.6.1
- * NetBSD version 1.6.2

Patch:

A patch is available via CVS:

<http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/uvm/uvm_swap.c.diff?r1=1.85&r2=1.85.2.1>

http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/uvm/uvm_swap.c.diff?r1=1.85&r2=1.85.2.1.

ADDITIONAL INFORMATION

The information has been provided by Evgeny Demidov.

Securiteam: [UNIX] NetBSD Kernel swapctl(2) DoS Vulnerability

=====

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.