

is this mbuf problem real?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-02/0093.html>

From: Baby Peanut (*baby_p_nut2_at_yahoo.com*)

Date: 02/18/04

Date: Wed, 18 Feb 2004 06:21:25 -0800 (PST)

To: freebsd-security@freebsd.org

BM_207650

MEDIUM

Vulnerability

Version: 1 2/18/2004@03:47:29 GMT

Initial report

<https://ialert.idefense.com/KODetails.jhtml?irId=207650>

ID#207650:

FreeBSD Memory Buffer Exhaustion Denial of Service Vulnerability (iDEFENSE Exclusive): Remote exploitation of a denial of service (DoS) vulnerability in FreeBSD's memory buffers (mbufs) could allow attackers to launch a DoS attack.

By sending many out-of-sequence packets, a low bandwidth denial of service attack is possible against FreeBSD. When the targeted system runs out of memory buffers (mbufs), it is no longer able to accept or create new connections.

Analysis: (iDEFENSE US) Exploitation of this vulnerability requires that the targeted system has at least one open TCP port.

The DoS will last until the port is closed, either by the attacker or the target machine.

Detection: iDEFENSE has confirmed this vulnerability exists in FreeBSD 5.1 (default install from media). It is expected that it also exists in earlier versions.

Exploit: iDEFENSE has proof of concept exploit code demonstrating the impact of this vulnerability.

Vulnerability Types: Design Error – Denial of Service

Prevalence and Popularity: Almost always

Evidence of Active Exploitation or Probing: No known exploitation or spike in probing

Ease of Exploitation: Remotely Exploitable

Existence and Availability of Exploit Code: An Exploit exists and is closely traded.

FreeBSD–Security: is this mbuf problem real?

Vulnerability Consequence: Availability

Do you Yahoo!?

Yahoo! Mail SpamGuard – Read only the mail you want.

<http://antispam.yahoo.com/tools>

freebsd–security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd–security>

To unsubscribe, send any mail to "freebsd–security–unsubscribe@freebsd.org"