

Apache vulnerability checking

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-06/0282.html>

From: Syzop (syz@dds.nl)

Date: 06/23/02

Date: Sun, 23 Jun 2002 12:00:34 +0200

From: Syzop <syz@dds.nl>

To: vuln-dev@securityfocus.com

Hi,

I've been checking sites for some time now with this attached prog (and mailing the webmasters), what it does is send a:

--

GET /checkapache.html HTTP/1.0

Transfer-Encoding: chunked

999999999; a 0

— request, and see what happens. Vulnerable apache: crashes, so connection is closed. Not vulnerable apache: sends something back IIS/some other things: waits for more data (?)

Anyway, I thought that when I'm sure it's an apache server ("Server: Apache blabla") and it crashes then it must be vulnerable. Is this always the case? This morning I received a mail from some admin who I had mailed and he told me they had already upgraded. Full server version: "Server: Apache/1.3.24 (Unix) (Red-Hat/Linux) mod_ssl/2.8.8 OpenSSL/0.9.6b mod_perl/1.26"

So my question is: has redhat changed something in the bad- chunked-encoding-detected-behavior in their backport or did this guy just forget to restart apache?

Btw, there are some other "major sites" which do also drop the connection but I couldn't see if they were running apache servers. www.tucows.com / www.geocities.com / www.yahoo.com / etc They do respond to "good" chunked encoding requests. Anyway I didn't mail them since it could be some weird http server behavior.

Cya,

Bram Matthys

- application/x-unknown-content-type-file attachment: [checkap.c](#)
-

- **Previous message:** [Michal Zalewski: "Re: Another flaw in Apache?"](#)

SecurityFocus Vuln-Dev: Apache vulnerability checking

- ***Next in thread:*** Toni Heinonen: "Re: Apache vulnerability checking"
- ***Reply:*** Toni Heinonen: "Re: Apache vulnerability checking"
- ***Reply:*** Elan Hasson: "RE: Apache vulnerability checking"
- ***Reply:*** Alex Balayan: "Re: Apache vulnerability checking"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]