

Securiteam: Re: elm bug ver 2.5.3 maybe others. (not suid on linux but suid on other OS.)

Re: elm bug ver 2.5.3 maybe others. (not suid on linux but suid on other OS.)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0141.html>

From: SecurITeam BugTraq Monitoring (bugtraq@securiteam.com)

Date: 02/25/02

From: "SecurITeam BugTraq Monitoring" <bugtraq@securiteam.com>

To: <vuln-dev@securityfocus.com>

Date: Mon, 25 Feb 2002 12:13:18 +0200

Hi,

Elm 2.5 PL6, of August 7, 2001 isn't affected as you can see:

```
# export EDITOR=`perl -e 'print "A" x 2000;`
```

```
# elm
```

Notice: ELM requires an ".elm" subdirectory off your home directory to hold information such as your configuration preferences (the "elmrc" file) and aliases.

May I create this directory for you (yes/no/quit) ? [y] : n

Very well, but you may run into difficulties later.

Nothing happens

I don't think my version is old enough to manifest this vulnerability.

Thanks

Noam Rathaus

<http://www.SecurITeam.com>

<http://www.BeyondSecurity.com>

----- Original Message -----

From: "Ehud Tenenbaum" <analyzer@2xss.com>

To: <vuln-dev@securityfocus.com>

Sent: Sunday, February 24, 2002 08:45

Subject: elm bug ver 2.5.3 maybe others. (not suid on linux but suid on other OS.)

> Hey,

>

> 2xs Security team found new bug in elm, although its not suid

> on linux systems(redhat 6.2, mandrak 8.0, slackware 7.1) we

> believe its suid on other kind of *nix OS such as HP-UX

Re: elm bug ver 2.5.3 maybe others. (not suid on linux but suid on other OS.)

Securiteam: Re: elm bug ver 2.5.3 maybe others. (not suid on linux but suid on other OS.)

```
>
> w00p@Analyzer:/tmp/w00p/elm2.5.3/bin$ id
> uid=100(w00p) gid=100(users) groups=100(users)
> w00p@Analyzer:/tmp/w00p/elm2.5.3/bin$
>
> w00p@Analyzer:/tmp/w00p/elm2.5.3/bin$ export EDITOR=`perl -e 'print "A"
> x 2000;`
> w00p@Analyzer:/tmp/w00p/elm2.5.3/bin$ elm
>
> Notice: ELM requires an ".elm" subdirectory off your home directory
> to hold information such as your configuration preferences (the
> "elmmc" file) and aliases.
>
> May I create this directory for you (yes/no/quit) ? [y] : n
> Segmentation fault
> w00p@Analyzer:/tmp/w00p/elm2.5.3/bin$
>
> w00p@Analyzer:/tmp/w00p/elm2.5.3/bin$ gdb ./elm
> GNU gdb 5.0
> Copyright 2000 Free Software Foundation, Inc.
> GDB is free software, covered by the GNU General Public License, and you
> are
> welcome to change it and/or distribute copies of it under certain
> conditions.
> Type "show copying" to see the conditions.
> There is absolutely no warranty for GDB. Type "show warranty" for
> details.
> This GDB was configured as "i386-slackware-linux"...
> (gdb) r
> Starting program: /tmp/w00p/elm2.5.3/bin/./elm
> warning: Unable to find dynamic linker breakpoint function.
> GDB will be unable to debug shared library initializers
> and track explicitly loaded dynamic code.
>
> Notice: ELM requires an ".elm" subdirectory off your home directory
> to hold information such as your configuration preferences (the
> "elmmc" file) and aliases.
>
> May I create this directory for you (yes/no/quit) ? [y] : n
>
> Program received signal SIGSEGV, Segmentation fault.
> 0x40074486 in catgets () from /lib/libc.so.6
> (gdb) where
> #0 0x40074486 in catgets () from /lib/libc.so.6
> #1 0x805b6a6 in create_private_dir ()
> #2 0x805b3fc in initialize ()
> #3 0x80520bd in main ()
> #4 0x4006faa7 in __libc_start_main () from /lib/libc.so.6
> (gdb) info registers
> eax 0x41414141 1094795585
> ecx 0x40014000 1073823744
```

Re: elm bug ver 2.5.3 maybe others. (not suid on linux but suid on other OS.)

Securiteam: Re: elm bug ver 2.5.3 maybe others. (not suid on linux but suid on other OS.)

> *edx 0x0 0*
> *ebx 0x4013bed4 1075035860*
> *esp 0xbfffe000 0xbfffe000*
> *ebp 0xbfffe004 0xbfffe004*
> *esi 0x41414141 1094795585*
> *edi 0xbffff264 -1073745308*
> *eip 0x40074486 0x40074486*
> *eflags 0x10202 66050*
> *cs 0x23 35*
> *ss 0x2b 43*
> *ds 0x2b 43*
> *es 0x2b 43*
> *fs 0x0 0*
> *gs 0x0 0*
> *fctrl 0x37f 895*
> *fstat 0x0 0*
> *ftag 0xffff 65535*
> *fiseg 0x0 0*
> *fioff 0x0 0*
> *foseg 0x0 0*
> *fofff 0xbffff8a4 -1073743708*
> *fop 0x0 0*
> *(gdb)*
>
> *Bug was found with BOS, Binary Overflow Scanner tool made*
> *by 2xs Security team.*
>
> *At this point we shall not release an exploit.*
> *For Questions or Comments:*
>
> *Ehud Tenenbaum <analyzer@2xss.com> CTO & Project manager.*
> *Izik Kotler <izik@2xss.com> Senior programmer.*
> *Mixer <[mixter@2xss.com](mailto:mixer@2xss.com)> Senior programmer.*
> *acz <acz@2xss.com> QA/Programmer.*
>
> --
> -----
> *Ehud Tenenbaum*
> *C.T.O & Project Manager*
> *2xs LTD.*
> *Tel: 972-9-9519980*
> *Fax: 972-9-9519982*
> *E-Mail: ehud@2xss.com*
> -----
> *Have A Safe Day*
>

-
- **Previous message:** [SecurITeam BugTraq Monitoring: "CGI.pm may assist in IDS evasion"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)