

[VulnWatch] Re: [xfocus-SD-060206]BCB compiler incorrect deal sizeof operator vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-02/msg00007.html>

- *From:* XFOCUS Security Team <security@xxxxxxxxxx>
 - *Date:* Tue, 07 Feb 2006 12:39:28 +0800
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

thank Ilja van Sprundel <ilja@xxxxxxxxxx> testing.
he find that newest tiny c compiler (tcc-0.9.23) also have this vulnerability .

also thank kokanin@xxxxxxxx and alekc@xxxxxxxx :)

/**

* check_compiler_sizeof_vulnerability.c

*

* Check compiler whether correct deal with sizeof operator,
* which can cause integer overflow if you careless use !!!

*

* note: some old compiler maybe have this vulnerability!!!!

*

* by alert7@xxxxxxxx

*

* XFOCUS Security Team

* <http://www.xfocus.org>

*

* already tested:

*

* BCB6+ent_upd4.....vuln !!!

* tcc-0.9.23vuln !!!

*thank Ilja van Sprundel <ilja@xxxxxxxxxx>

* gcc version 4.0.0 20050519 (Red Hat 4.0.0-8).....not vuln

* gcc version 2.95.3-4(cygwin special).....not vuln

* gcc version egcs-2.91.66.....not vuln

* cc: Sun WorkShop 6 2000/04/07 C 5.1not vuln

* VC6+sp5.....not vuln

*thank eyas

* lcc version 3.8.....not vuln

*thank tombkeeper

* evc4+sp4.....not vuln

[VulnWatch] Re: [xfocus-SD-060206]BCB compiler incorrect deal sizeof operator vulnerability

*thank san
* gcc version 3.4.2 [FreeBSD] 20040728.....not vuln
*thank <kokanin@xxxxxxxx>
* GCC OpenBSD 3.1 (2.95.3 20010125 (prerelease))...not vuln
* MS VS.NET 2003not vuln
*above two thank <alekc@xxxxxxxx>
*

* REQUEST YOUR COMMENT:
* VC6 not sp5.....?
* VC7.....?
* evc not sp4.....?
* ...
*/

#include <stdio.h>

```
int main(int argc, char *argv[])  
{  
int i=-1;
```

```
printf("Check compiler whether correct deal with sizeof operator\n");  
printf(" by alert7@xxxxxxxx \n\n");
```

```
if (i > sizeof ( int ) )  
{  
printf("This compiler is not vuln\n");  
}else  
printf("This compiler is vuln!!!\n");
```

```
getchar();
```

```
return 0;  
}
```

--EOF

Kind Regards,

XFOCUS Security Team
<http://www.xfocus.org>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.1 (GNU/Linux)

iD8DBQFD6CR/whDwaF6cSWIRArcqAKCmTor93qg3JlmPEL6VjMHZgGI7hgCgxwtM
r71nRPE+00IBZW0hSqjEnU4=
=Bl/T

[VulnWatch] Re: [xfocus-SD-060206]BCB compiler incorrect deal sizeof operator vulnerability 2

[VulnWatch] Re: [xfocus-SD-060206]BCB compiler incorrect deal sizeof operator vulnerability

-----END PGP SIGNATURE-----