TEAM INTELL

Varuhi vaše mreže
Guardians of your network

Security Advisory TISA2007-07-Public

iBON 2006 memory corruption

Release date:	30.07.2007
Severity:	Less critical
Impact:	Memory Corruption / DoS
Status:	Official patch available
Software:	iBON 2006
Tested on:	Microsoft Windows Professional XP SP2
Vendor:	http://www.ibon.com
Disclosed by:	Edi Strosar (TeamIntell)

Summary:

iBON 2006 is subject to memory corruption bug that results in local denial of service (DoS). This issue is due to the application's failure to properly bounds-check user supplied input before copying it to an insufficiently sized memory buffer.

Analysis:

iBON is a computer organized database of prudential reports and financial information gathered on a CD-ROM for Slovenian business subjects. The application is prone to memory corruption bug which may be triggered by entering > 32.800 chars into search input field within iBON GUI. This will result in arbitrary memory write attempt that leads to local denial of service (application hang, 100% CPU usage, general system unresponsiveness).

The bug is confirmed in iBON 2006 and prior. iBON 2007 (latest version) is not affected.

Debugger output:

```
(d10.a50): Access violation - code c0000005 (first/second chance not available)
eax=077c1bcc ebx=0771ecfc ecx=000003ef edx=00008003 esi=00001300 edi=0771ecfc
eip=00401fe6 esp=0189febc ebp=0189fee8 iopl=0         nv up ei ng nz na pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000287
*** ERROR: Module load completed but symbols could not be loaded for Ibon.exe
Ibon+0x1fe6:
00401fe6 895a04          mov     dword ptr [edx+4],ebx ds:0023:00008007=????????
```

Solution:

Update to latest version.

Timeline:

25.07.2007 – Vulnerability discovered
27.07.2007 – Vendor informed
30.07.2007 – Public disclosure

Contact:

Maldin d.o.o.
Tržaška cesta 2
1000 Ljubljana - SI
tel: +386 (0)590 70 170
fax: +386 (0)590 70 177
gsm: +386 (0)31 816 400
web: www.teamintell.com
e-mail: info@teamintell.com

Disclaimer:

The content of this report is purely informational and meant for educational purposes only. Maldin d.o.o. shall in no event be liable for any damage whatsoever, direct or implied, arising from use or spread of this information. Any use of information in this advisory is entirely at user's own risk.