TEAM INTELL

Varuhi vaše mreže
Guardians of your network

Security Advisory TISA2007-03-Public

PIRS 2007 local buffer overflow vulnerability

Release date:	13.7.2007
Severity:	Less critical
Impact:	Buffer overflow
Status:	Official patch available
Software:	PIRS 2007 (CD version)
Tested on:	Microsoft Windows Professional XP SP2
Vendor:	http://www.pirs.si
Disclosed by:	Edi Strosar (TeamIntell)

Summary:

Poslovni informator Republike Slovenije (PIRS) 2007 is vulnerable to local buffer overflow. It might be possible to execute arbitrary code in a context of currently logged on user. Direct remote code execution is not possible.

Analysis:

PIRS is a data collection of companies and other active business subjects in Slovenia. The main application **pirs32.exe** contains buffer overflow that may allow code execution. Input validation is not performed on search parameter lenght which leads to overflow condition. Entering =>528 ASCII characters in any input/search field within PIRS GUI will cause application to silenty crash.

Proof of concept:

The following string **512*A** + **4*B** + **8*A** + **4*C** will overwrite **ECX** and **EIP** registers. EIP is the pointer to location where the next instruction will be executed.

Note: because pirs32.exe silently crashes the PoC must be reproduced inside debugger.

Solution:

Vendor has released a patch that limits the maximum search string lenght to 255 characters.

Download link:
http://www.pirs.si/slo/index.php?dep_id=29&help_id=60

Timeline:

24.06.2007 – vulnerability discovered
25.06.2007 – vendor informed
13.07.2007 – patch released
13.07.2007 – 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.