# Security Advisory TISA2007-08-Public

## Birokrat heap corruption (heap overflow)

| | |
|---|---|
| **Release date:** | 31.07.2007 |
| **Severity:** | Less critical |
| **Impact:** | Heap Corruption / Heap Overflow |
| **Status:** | Unpatched |
| **Software:** | Birokrat (version 7.4) |
| **Tested on**: | Microsoft Windows Professional XP SP2 |
| **Vendor:** | http://www.andersen.si<br>http://www.birokrat.si |
| **Disclosed by:** | Edi Strosar (Team Intell) |

### Summary:

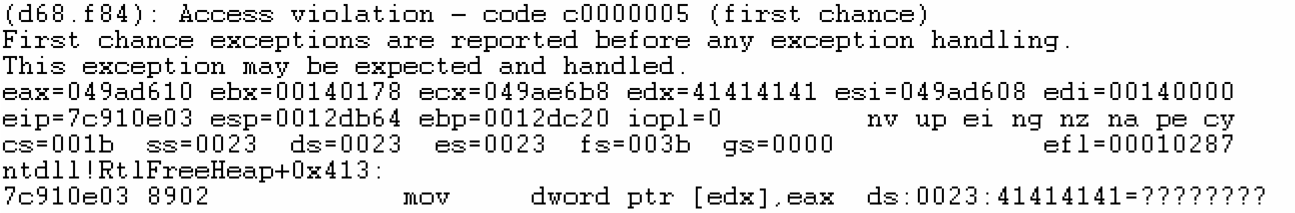
Birokrat is subject to heap corruption bug that may lead to local arbitrary code execution. The application fails to perform adequate boundary checks on user supplied input before copying it to an insufficiently sized memory buffer.

### Analysis:

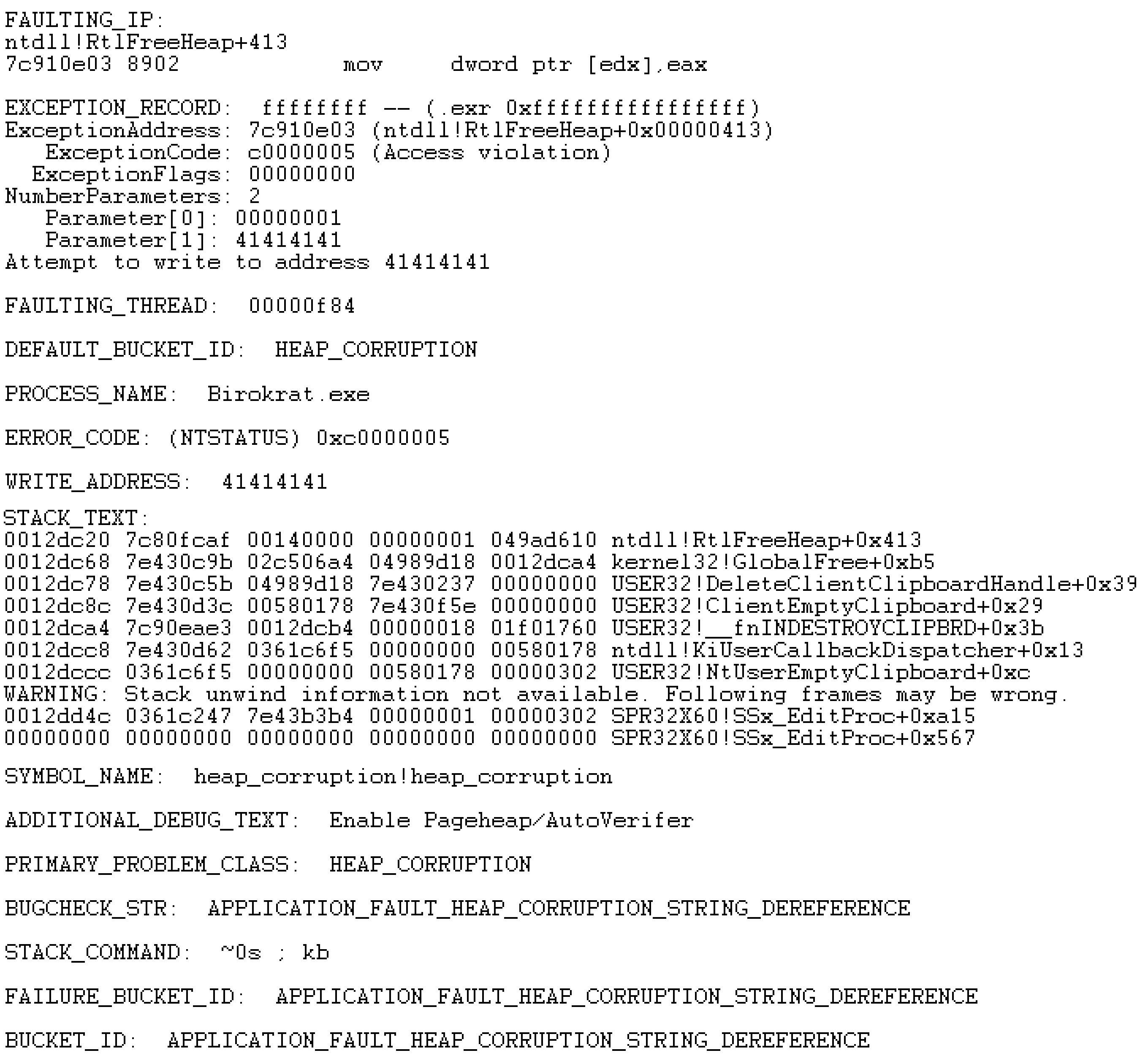
Birokrat is Slovenian business management software. The main application **birokrat.exe** is prone to heap-based overflow caused by improper bounds checking. Submitting overly long argument into affected input field, local users could overflow heap memory segment and possibly execute arbitrary code in the context of currently logged on user.

The bug is confirmed in Birokrat version 7.4.0797. Other versions may be affected.

### Debugger output:



```
(d68.f84): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=049ad610 ebx=00140178 ecx=049ae6b8 edx=41414141 esi=049ad608 edi=00140000
eip=7c910e03 esp=0012db64 ebp=0012dc20 iopl=0         nv up ei ng nz na pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010287
ntdll!RtlFreeHeap+0x413:
7c910e03 8902            mov     dword ptr [edx],eax  ds:0023:41414141=????????
```



```
FAULTING_IP:
ntdll!RtlFreeHeap+413
7c910e03 8902            mov     dword ptr [edx],eax

EXCEPTION_RECORD:  ffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 7c910e03 (ntdll!RtlFreeHeap+0x00000413)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 00000001
   Parameter[1]: 41414141
Attempt to write to address 41414141

FAULTING_THREAD:  00000f84

DEFAULT_BUCKET_ID:  HEAP_CORRUPTION

PROCESS_NAME:  Birokrat.exe

ERROR_CODE: (NTSTATUS) 0xc0000005

WRITE_ADDRESS:  41414141

STACK_TEXT:
0012dc20 7c80fcaf 00140000 00000001 049ad610 ntdll!RtlFreeHeap+0x413
0012dc68 7e430c9b 02c506a4 04989d18 0012dca4 kernel32!GlobalFree+0xb5
0012dc78 7e430c5b 04989d18 7e430237 00000000 USER32!DeleteClientClipboardHandle+0x39
0012dc8c 7e430d3c 00580178 7e430f5e 00000000 USER32!ClientEmptyClipboard+0x29
0012dca4 7c90eae3 0012dcb4 00000018 01f01760 USER32!__fnINDESTROYCLIPBRD+0x3b
0012dcc8 7e430d62 0361c6f5 00000000 00580178 ntdll!KiUserCallbackDispatcher+0x13
0012dccc 0361c6f5 00000000 00580178 00000302 USER32!NtUserEmptyClipboard+0xc
WARNING: Stack unwind information not available. Following frames may be wrong.
0012dd4c 0361c247 7e43b3b4 00000001 00000302 SPR32X60!SSx_EditProc+0xa15
00000000 00000000 00000000 00000000 00000000 SPR32X60!SSx_EditProc+0x567

SYMBOL_NAME:  heap_corruption!heap_corruption

ADDITIONAL_DEBUG_TEXT:  Enable Pageheap/AutoVerifer

PRIMARY_PROBLEM_CLASS:  HEAP_CORRUPTION

BUGCHECK_STR:  APPLICATION_FAULT_HEAP_CORRUPTION_STRING_DEREFERENCE

STACK_COMMAND:  ~0s ; kb

FAILURE_BUCKET_ID:  APPLICATION_FAULT_HEAP_CORRUPTION_STRING_DEREFERENCE

BUCKET_ID:  APPLICATION_FAULT_HEAP_CORRUPTION_STRING_DEREFERENCE
```

**Solution:**

Unpatched. Vendor not informed.

**Note:** Accordingly to our disclosure policy, we do not report bugs to Andersen.

**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.