

[Full-disclosure] Multiple vulnerabilities in Sauerbraten engine 2006_02_28

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-03/msg00131.html>

- From: Luigi Auriemma <aluigi@xxxxxxxxxxxxxx>
- Date: Mon, 6 Mar 2006 21:29:51 +0100

#####

Luigi Auriemma

Application: Sauerbraten engine

<http://sauerbraten.org>

Versions: <= 2006_02_28 and current CVS

Platforms: Windows, *nix, *BSD and MacOS

Bugs: A] sgetstr() buffer-overflow

B] invalid memory access

C] clients crash through invalid map

D] crash through unconnected client

Exploitation: remote, versus both server and clients

Date: 06 Mar 2006

Author: Luigi Auriemma

e-mail: aluigi@xxxxxxxxxxxxxx

web: <http://aluigi.altervista.org>

#####

- 1) Introduction
- 2) Bugs
- 3) The Code
- 4) Fix

#####

=====
 1) Introduction
 =====

Sauerbraten is the evolution of the Cube engine
 (<http://www.cubeengine.com>) developed by Wouter van Oortmerssen

(<http://strlen.com>), in fact can be defined also as "Next-Gen Cube" or "Cube 2".

It supports both LAN and Internet multiplayer through its master server.

#####

=====

2) Bugs

=====

----- A) sgetstr() buffer-overflow -----

The game uses an unchecked function for reading the strings from the incoming data.

The function is sgetstr() located in shared/cube.h:

```
#define sgetstr() { char *t = text; do { *t = getint(p); } while(*t+  
+); }
```

The problem, which affects both server and clients, is that this code copies the input data over the text buffer of size MAXTRANS (5000 bytes) allowing possible malicious code execution.

----- B) invalid memory access -----

sgetstr(), getint() and the instructions which call them don't check the correct length of the input data.

In short is possible to force the server or the client to read over the received data reaching unallocated zones of the memory and so crashing immediately.

----- C) clients crash through invalid map -----

In the Sauerbraten engine the players have the possibility to choose a specific map on which playing, if there is only one player in the server the map is changed immediately otherwise will be voted.

When a client tries to load an invalid map file it exits immediately showing the "while reading map: header malformed" error.

When the map is choosed all the clients add a .ogz extension to the mapname received from the server and load the file.

The max size of the mapname is 260 bytes and the function which loads

the file uses a secure sprintf() which truncates the input mapname (.ogz included) when the limit is reached.

Then the loading of the map is not sanitized versus possible directory traversal exploitations so if an attacker (a player) specifies a mapname of about 260 bytes he can force any client which will join the server (due to the voting problem explained previously which limits the exploitation of this bug) to load any file which is not a valid map and so they will exit immediately.

As already said the exploitation happens with any new client which joins the server since the new mapname will remain active in the server for all the current match.

D) crash through unconnected client

A partially connected client can easily crash the Sauerbraten server. This bug is caused by the following instruction in engine/server.cpp:

```
int num = ((client *)event.peer->data)->num;
```

In short when the connection times out the server tries to show the host of the disconnected client ignoring that it has never joined. The effect is the reading of an unallocated zone of the memory.

#####

=====
3) The Code
=====

<http://alugi.altervista.org/poc/sauerburn.zip>

#####

=====
4) Fix
=====

The developers will release a fix, only for the buffer-overflow bug, soon.

#####

Luigi Auriemma
<http://luigi.altervista.org>

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>