

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Cytel Studio 9.0.0 - Multiple Vulnerabilities

EDB-ID:

17930

CVE:

EDB Verified: ✓

Author:

[LUIGI AURIEMMA](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2011-10-04

Vulnerable App:





#####

Luigi Auriemma

Application: Cytel Studio: StatXact / LogXact / CrossOver
<http://www.cytel.com/Software/LogXact.aspx>
<http://www.cytel.com/Software/StatXact.aspx>
<http://www.cytel.com/Software/Crossover.aspx>

Versions: <= 9.0.0

Platforms: Windows

Bugs: A] strings stack overflow
 B] rows integer overflow
 C] CYB USE stack overflow

Exploitation: file

Date: 02 Oct 2011

Author: Luigi Auriemma
 e-mail: aluigi@autistici.org
 web: aluigi.org

#####

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

#####

=====

- 1) Introduction

=====

From vendor's website:

"Cytel, the acknowledged leader in exact statistical methods, helped pioneer exact methods for binary logistic regression and multinomial regression."

"First introduced in 1987, LogXact is unequivocally the fastest and most powerful logistic regression analysis software available today."

"With StatXact, Cytel's own powerful algorithms make exact inferences by permuting the actually observed data, eliminating the need for distributional assumptions."

#####

=====

- 2) Bugs

=====

 A] strings stack overflow

Buffer overflow during the copying of the strings in a stack buffer of 256 bytes.

 B] rows integer overflow

There is an integer overflow in the handling of the rows.

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

The number of rows (first element of the second line in the file) is multiplied by the size of the elements (8 for floats, 4 for strings and so on) and the allocated memory gets overflowed when the elements are copied one by one.

At the moment I have not seen ways to exploit this vulnerability to execute code so I report it just as reference.

Both the A and B problems are exploitable with the CY3 ("StatXact 5.0 data") and the CYL ("LogXact data") files.

C] CYB USE stack overflow

Stack overflow in the handling of the USE command of the CYB files.

#####

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

http://aluigi.org/poc/cytel_1.zip
<https://gitlab.com/exploit-database/exploitdb-bin-splotts/-/raw/main/bin-splotts/17930.zip>

#####

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

No fix.

#####

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

[OffSec Services Limited](#) 2026. All rights reserved.