Mestrado em Engenharia Informática (MEI)
Mestrado Integrado em Engenharia Informática (MiEI)

Perfil de Especialização **CSI** : Criptografia e Segurança da Informação

Engenharia de Segurança

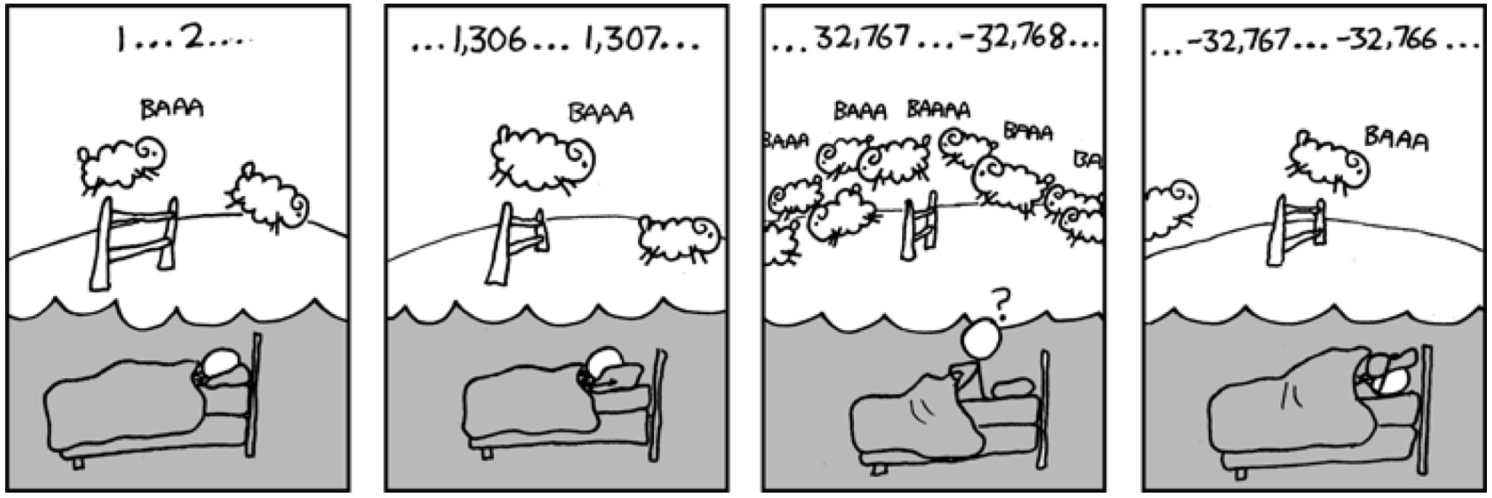
jose.miranda@devisefutures.com

Topics

- Integers Vulnerability

Integer error

- Too large or too small values of integers may fall outside the range of the data type, leading to undefined behavior that may reduce the robustness of the code as well as give rise to security vulnerabilities.
- For example, a 32-bit **int** may contain values from -2^{31} through $2^{31}-1$.
- An Integer error can lead to unexpected behavior or can be exploited to cause a program to crash, corrupt data, lead to incorrect behavior, or allow malicious software to run.



Integer error

CVE ID	Vulnerability type	Publish Date	CVSS Score	Description
CVE-2019-9210	Integer Overflow or Wraparound	2019-02-27	7.8	In AdvanceCOMP 2.1, png_compress in pngex.cc in advpng has an integer overflow upon encountering an invalid PNG size, which results in an attempted memcpy to write into a buffer that is too small. (There is also a heap-based buffer over-read.)
CVE-2019-3857	Integer Overflow or Wraparound	2019-03-25	8.8	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2018-6543	Integer Overflow or Wraparound	2018-02-02	7.8	In GNU Binutils 2.30, there's an integer overflow in the function load_specific_debug_section() in objdump.c, which results in `malloc()` with 0 size. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2016-3074	Denial Of Service Execute Code Overflow	2016-04-26	7.5	Integer signedness error in GD Graphics Library 2.1.1 (aka libgd or libgd2) allows remote attackers to cause a denial of service (crash) or potentially execute arbitrary code via crafted compressed gd2 data, which triggers a heap-based buffer overflow.
CVE-2018-6543	DoS Overflow	2018-02-02	6.8	In GNU Binutils 2.30, there's an integer overflow in the function load_specific_debug_section() in objdump.c, which results in `malloc()` with 0 size. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-7471	Overflow	2018-02-25	7.5	KingView 7.5SP1 has an integer overflow during stgopenstorage API read operations.

Integer error

- Most Unix systems store the date/time in a variable of type 32-bit int – the date/time is saved as the number of seconds since 00h00 on Jan 1, 1970. On 19/Jan/2038, the overflow of this variable occurs, passing the date/time to be negative. More information at http://en.wikipedia.org/wiki/Year_2038_problem

Integer error

- On Facebook there is a group that states the following:

  - Why do they say that?
  - What are the potential problems if this happens?

Integer error

- YouTube could not stand the Gangnam Style

The Economist explains

How "Gangnam Style" broke YouTube's counter

The powers of two permeate computing, but only pop out at odd times

The Economist explains ›
Dec 10th 2014 | by G.F. | SEATTLE

THE popularity of the "Gangnam Style" video by Psy, a South Korean pop star, is beyond all reckoning. Or at least it was, until a change was made in YouTube's programming. The singer's video was poised to exceed 2,147,483,647 plays, at which point YouTube would have been unable to count any higher. But the boffins made some tweaks, and now Psy is safe until his rousing anthem passes over nine quintillion views: 9,223,372,036,854,775,808 to be precise. Why couldn't YouTube count high enough?

Integer error

- On 25 December 2004, the airline Comair airlines was forced to keep 1,100 flights on the ground after the crew scheduling software collapsed. The software used a 16-bit integer (maximum 32,768) to number the crew changes for a month, with that number being exceeded that month due to bad weather that led to numerous crew changes.

FEATURE

Comair's Christmas Disaster: Bound To Fail

The 2004 crash of a critical legacy system at Comair is a classic risk management mistake that cost the airline $20 million and badly damaged its reputation.

By Stephanie Overby

CIO | MAY 1, 2005 8:00 AM PT

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULT

UNCATEGORIZED —

Comair/Delta airline debacle caused by the overflow of 16-bit pointer

One of the most nightmarish Christmas travel foul-ups in recent memory was ...

CLINT ECKER - 12/30/2004, 7:24 PM

Integer error – truncation problem

- On 4 June 1996, the unmanned Ariane 5 rocket exploded 40 seconds after launch. The rocket was making its first voyage after a decade of development costing about $ 7 billion, the rocket being destroyed and its cargo were valued at $ 500 million.
- The cause of the explosion was a software error in the inertial reference system. More specifically, a 64-bit float number related to the horizontal rocket velocity was converted to a signed 16-bit integer. The number to convert was greater than 32,767 (largest integer that can be saved in a signed int), so the conversion failed.

Integer error

- Risk
  - Declaring a variable with a particular type allocates a fixed memory space. Most languages allow you to declare several types of integers (short, int, long, etc.). For example, a 32-bit int can store values between -2^{31} (-2 147 483 648) and $2^{31}-1$ (2 147 483 647).
  - Often the size of the data types are machine and compiler dependent ...
- ”Responsible” codification
  - Knowing the limits: as the size of the data type is dependent on the machine and compiler it is a good idea to familiarize yourself with the limits on the machine where the program will run;
  - Data Type: Choose the type of integer best suited for the values it will contain, in the programming language you are using;
  - Validate the input: (more detailed in the next section);
  - Validate possible overflows/underflows before operations on integers;
  - Configure compiler parameters: options that check for potential errors;
  - Use specific libraries: for example, the SafeInt class in C ++.