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

Integers vulnerability

The CWE Top 25

Below is a brief listing of the weaknesses in the 2019 CWE Top 25, including the overall score of each.

Rank	ID	Name	Score
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	CWE-20	Improper Input Validation	43.61
[4]	CWE-200	Information Exposure	32.12
[5]	CWE-125	Out-of-bounds Read	26.53
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	CWE-416	Use After Free	17.94
[8]	CWE-190	Integer Overflow or Wraparound	17.35

https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

Integers vulnerability

CWE-190: Integer Overflow or Wraparound

Weakness ID: 190
Abstraction: Base
Structure: Simple

Status: Stable

Presentation Filter: Complete

Description

The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control.

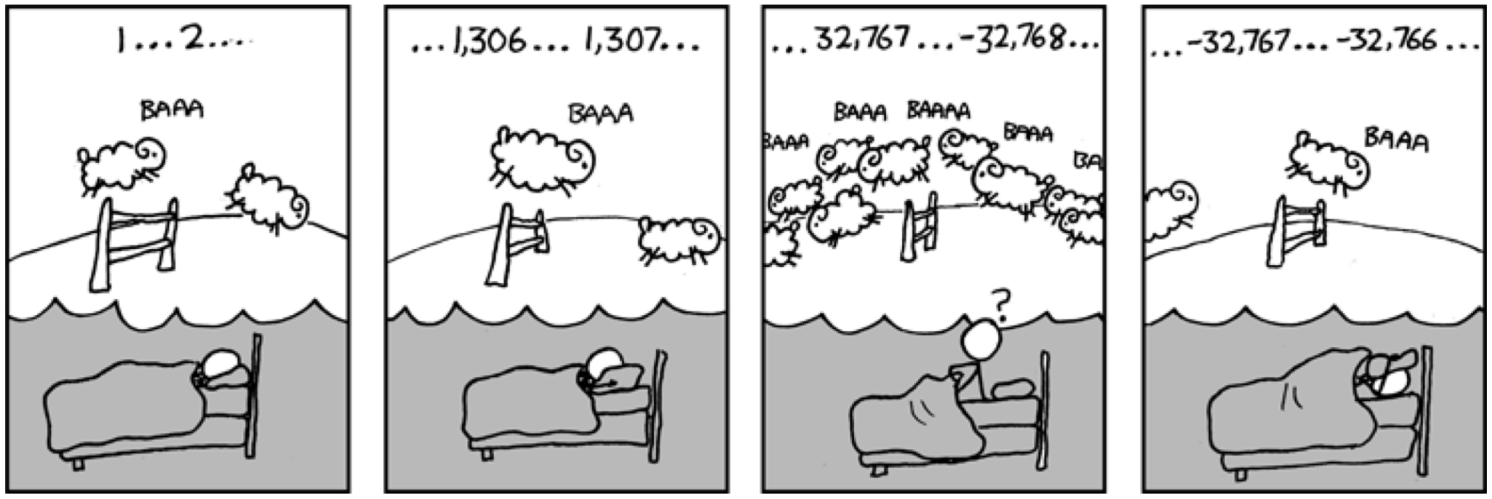
Extended Description

An integer overflow or wraparound occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may wrap to become a very small or negative number. While this may be intended behavior in circumstances that rely on wrapping, it can have security consequences if the wrap is unexpected. This is especially the case if the integer overflow can be triggered using user-supplied inputs. This becomes security-critical when the result is used to control looping, make a security decision, or determine the offset or size in behaviors such as memory allocation, copying, concatenation, etc.

https://cwe.mitre.org/data/definitions/190.html

Integer overflow

- 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 overflow

CVE ID	Vulnerability type	Publish Date	CVSS Score	Description
CVE-2020-6381	Integer Overflow or Wraparound	2020-02-11	8.8	Integer overflow in JavaScript in Google Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-8874	Integer Overflow or Wraparound	2020-03-23	7.5	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor.
CVE-2019-9257	Integer Overflow or Wraparound	2019-09-27	7.8	In Bluetooth, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10
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-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.

Integer overflow

- Most Unix and embedded 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

Binary : 01111111 11111111 11111111 11110000
Decimal : 2147483632
Date : 2038-01-19 03:13:52 (UTC)
Date : 2038-01-19 03:13:52 (UTC)

Integer overflow

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

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

Integer overflow

- 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 overflow

- 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 32,767) 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 —

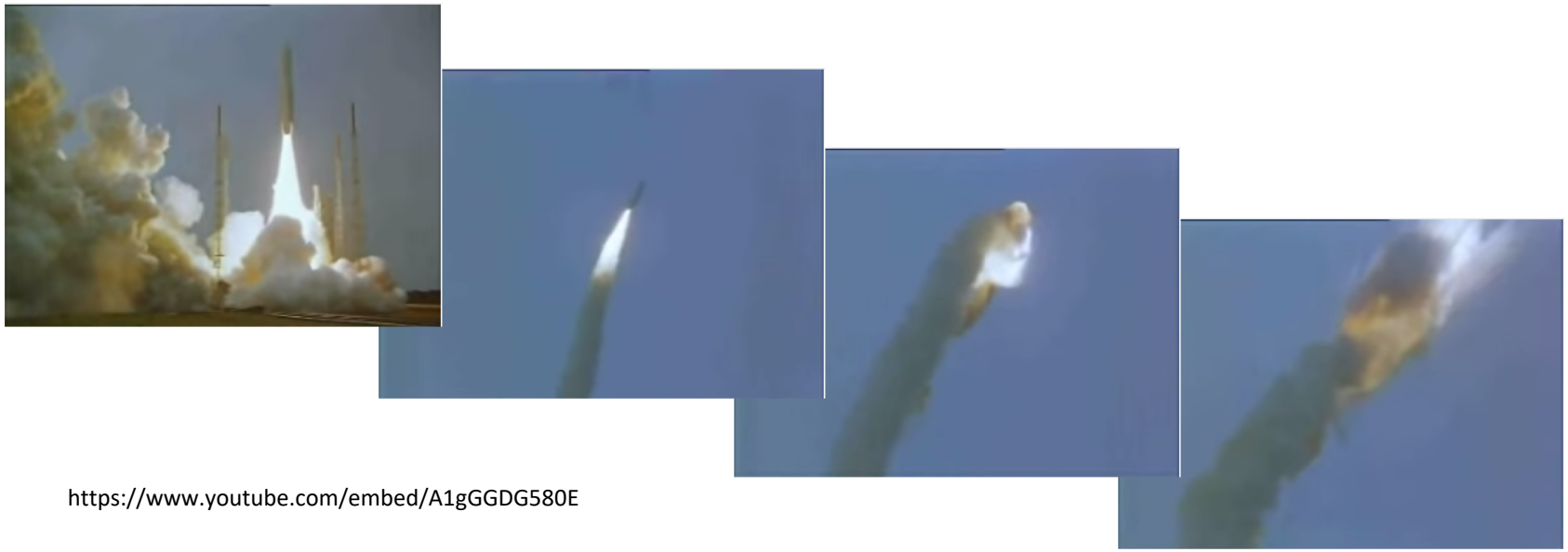
Comair/Delta airline debacle caused by the overflow of 16-bit pointer

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

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

Integer overflow – 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.



https://www.youtube.com/embed/A1gGGDG580E

Integer overflow

- 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 ++.