



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

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

Engenharia de Segurança

Tópicos de Segurança de Software

- Vulnerabilidade de Inteiros



Vulnerabilidade de Inteiros

The CWE Top 25

Below is a brief listing of the weaknesses in the 2021 CWE Top 25, including the overall score of each.

Rank	ID	Name	Score	2020 Rank Change
[1]	CWE-787	Out-of-bounds Write	65.93	+1
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.84	-1
[3]	CWE-125	Out-of-bounds Read	24.9	+1
[4]	CWE-20	Improper Input Validation	20.47	-1
[5]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19.55	+5
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19.54	0
[7]	CWE-416	Use After Free	16.83	+1
[8]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.69	+4
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	14.46	0
[10]	CWE-434	Unrestricted Upload of File with Dangerous Type	8.45	+5
[11]	CWE-306	Missing Authentication for Critical Function	7.93	+13
[12]	CWE-190	Integer Overflow or Wraparound	7.12	-1

https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html

Vulnerabilidade de Inteiros

CWE-190: Integer Overflow or Wraparound

Weakness ID: 190

Abstraction: Base

Structure: Simple

Status: Stable

Presentation Filter: 

▼ 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.

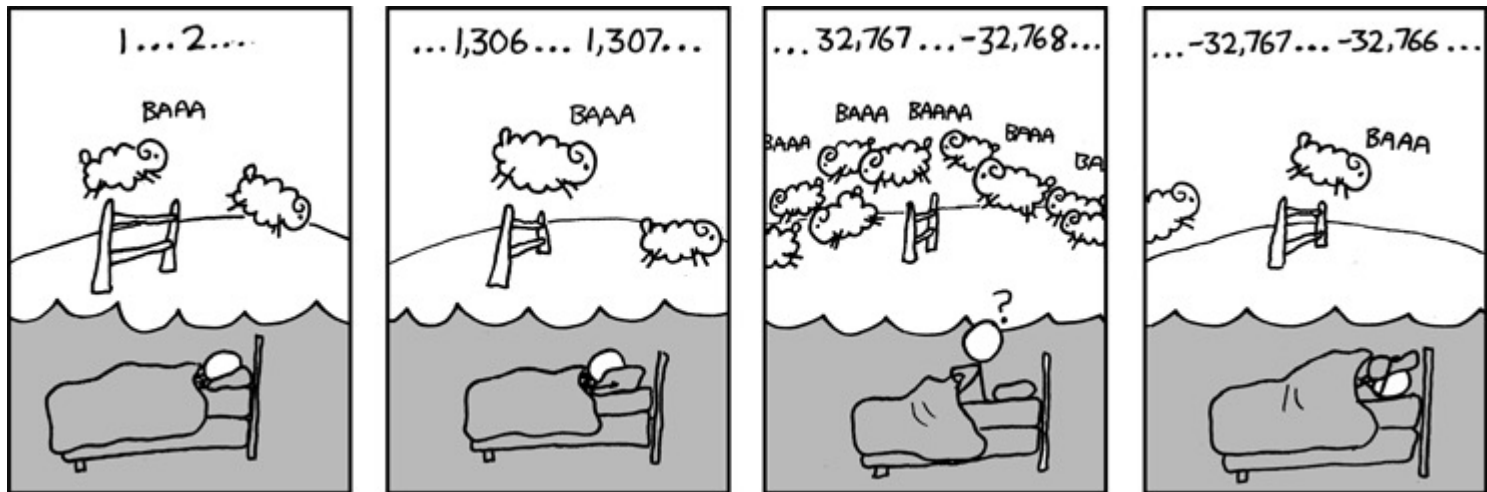
▼ Extended Description

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

- Valores muito grandes ou muito pequenos de inteiros podem cair fora do intervalo do tipo de dados, levando a um comportamento indefinido que pode reduzir a robustez do código, assim como dar origem a vulnerabilidades de segurança.
- Por exemplo, um int de 32-bit pode conter valores de -2^{31} até $2^{31}-1$.
- Um erro de Inteiros pode levar a comportamento inesperado ou, pode ser explorado para causar o *crash* de um programa, corromper dados, levar a comportamento incorreto ou permitir a execução de software malicioso.





Integer overflow

CVE ID	Vulnerability type	Publish Date	CVSS Score	Description
CVE-2022-29175	Integer Overflow or Wraparound	2022-05-05	9.8	Vyper is a pythonic smart contract language for the ethereum virtual machine. Since version 0.3.2, decimals use the full range of the underlying int168 type. multiplication of 168 bit integers can wrap in 256-bit arithmetic, but safemul does not check for that. This has been patched in v0.3.4. There are no known workarounds for this issue.
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	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

- A maior parte dos sistemas Unix e *embedded systems* (sector automóvel, militar, médico, aviação, ...) guarda a data/hora numa variável do tipo int 32-bit – a data/hora é guardada como o número de segundos desde as 00h00 de 1/Jan/1970. A 19/Jan/2038, ocorre o overflow dessa variável, passando a data/hora a ser negativa. Mais informação em 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

- No Facebook existe um grupo que afirma o seguinte:



- Porque é que afirmam isso?
- Quais seriam os potenciais problemas se isso ocorresse?

Integer overflow

- YouTube não aguentou o Gangnam Style

YouTube não aguentou o *Gangnam Style*

PÚBLICO 03/12/2014 - 16:38

É o próprio site a confirmar que teve problemas. "*Gangnam Style* foi visto tantas vezes que tivemos que fazer um *upgrade*."

É o próprio site a confirmar que teve problemas. "*Gangnam Style* foi visto tantas vezes que tivemos que fazer um *upgrade*", escreve o YouTube na sua página no Google+.

Se passarmos o cursor sobre o contador que se pode ver na página do vídeo este não pára de rodar e isso porque o YouTube nunca pensou que um tal número pudesse vir a ser atingido. "Nunca pensámos que um vídeo pudesse ser visto em números mais do que um número inteiro de 32-bit (=2.147.483.647 visualizações), mas isso foi antes de termos conhecido Psy", admite o YouTube.

Integer overflow

- No dia 25 Dezembro 2004, a companhia aérea *Comair airlines* foi forçada a manter no solo 1.100 voos após o software de agendamento das tripulações colapsar. O software utilizava um inteiro de 16-bit (máximo 32.767) para numerar as alterações de tripulação durante um mês, tendo esse número sido excedido nesse mês devido a mau tempo que levou a inúmeras alterações de tripulação.

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 – problema de truncamento

- A 4 de Junho de 1996, o foguetão não tripulado Ariane 5 explodiu 40 segundos depois do lançamento. O foguetão fazia a sua primeira viagem após uma década de desenvolvimento, com custos na ordem dos \$7 biliões, estando o foguetão destruído e a sua carga avaliada em \$500 milhões.
- A causa da explosão foi um erro de software no sistema de referência de inércia. Mais especificamente, um número *float* de 64 bits relacionado com a velocidade horizontal do foguetão, foi convertido num inteiro de 16 bits (*signed int*). O número a converter era maior do que 32.767 (maior inteiro que pode ser guardado num *signed int*), pelo que a conversão falhou.



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

Integer overflow

- Risco
 - Declarar uma variável com determinado tipo aloca um espaço fixo de memória. A maior parte das linguagens permite declarar diversos tipos de inteiros (short, int, long, etc.). Por exemplo, um int de 32 bits pode guardar valores entre -2^{31} (-2 147 483 648) e $2^{31}-1$ (2 147 483 647).
 - Muitas vezes, o tamanho dos tipos de dados são dependentes da máquina e do compilador ...
- Codificação “responsável”
 - Conhecer os limites: como o tamanho do tipo de dados é dependente de máquina e compilador é uma boa ideia familiarizar-se com os limites na máquina onde o programa vai executar;
 - Tipo de dados: escolha o tipo de inteiro mais adequado para os valores que vai conter, na linguagem de programação que está a utilizar;
 - Validar o input: (mais detalhado na próxima secção);
 - Validar possíveis overflows/underflows antes de operações sobre inteiros; 
 - Configurar parâmetros do compilador: opções que verificam potenciais erros;
 - Utilizar bibliotecas específicas: por exemplo, a classe SafeInt no C++.