Lessons learned –
PISEA 2022 - Ergebnis in Safety und IT-Security

(*PISEA – a Programme for International Science and Engineering Assessment 2022*)

Hubert B. Keller
CEO ci-tec GmbH, Karlsruhe (www.ci-tec.de)
Independent Expert in Safe&Secure Software, Real Time Systems,
Machine Intelligence, Software Engineerin, Ada - The programming language

8. Berliner Gesamtkonferenz der Sicherheitsinstitutionen, 21. Oktober 2022, Berlin

Berliner Gesamtkonferenz der Sicherheitsinstitutionen

Agenda

Lessons learned – PISEA Ergebnis in Safety und IT-Security
(PISEA – a Programme for International Science and Engineering Assessment)
oder

Was haben wir (**nicht**) gelernt in der Entwicklung von Cyber Scurity
für Software-Systeme.

- Zur Person
- CVE / CWE Definitionen
- Zur Situation
- Ursachen (Vulnerabilities im Deatil)
- Aspekte für Security
- Akteure und Aktivitäten
- Resümee

Berliner Gesamtkonferenz der Sicherheitsinstitutionen

Zur Person

- **Dr. Hubert B. Keller**
  - Forschung/Beratung in Sichere Software, Echtzeitsysteme, Maschinelle Intelligenz, Software Engineering
  - CEO ci-tec GmbH, Karlsruhe
  - Dozent DHBW, Karlsruhe
  - Mitbegründer GI Fachbereich Sicherheit – Schutz und Zuverlässigkeit
  - Mitautor „Technical Safety – An Attribute of Quality. Springer 2018
    Autor von „Maschinelle Intelligenz“, Vieweg Verlag, 2000,
    Autor von „Echtzeitsysteme“, Springer Verlag, 2019
  - Mit-Initiator Berliner Sicherheitskonferenz
  - Co-Chair Sicherheitstagung GI 2003, Reliable Software Technologies Europe Konferenz 2000 und 2013
  - Bis 2021
    Leiter Fachgebiet „Advanced Automation Technologies“ am KIT mit Security Lab Energy und KASTEL
    Dozent für Technische Informatik

Mitbegründer des Fachbereichs Sicherheit der Gesellschaft für Informatik

Förderverein
Ada
Deutschland e. V.

Vorsitzender von
Ada Deutschland e.V.
(Verein für sichere Software)

ci-tec GmbH, Karlsruhe

ci-tec

- Gegründet 2001
- Firmensitz Karlsruhe
- 10 Angestellte

ci-tec
GmbH

Forschung & Entwicklung

Projekte in Zusammenarbeit mit

- Universitäten (z. B. KIT)
- Unternehmen (z. B. BASF)

Förderung durch BMBF, BMWi, BW u.a.

- aktuell 3 DoktorandInnen

Schutzrechte

Industrie

Kunden aus den Bereichen

- Zementherstellung
- Siliziumherstellung
- Sonderabfallverwertung
- (Zink-) Recycling
- Hausmüllverwertung

> 100 Installationen weltweit (Europa, Asien, …)

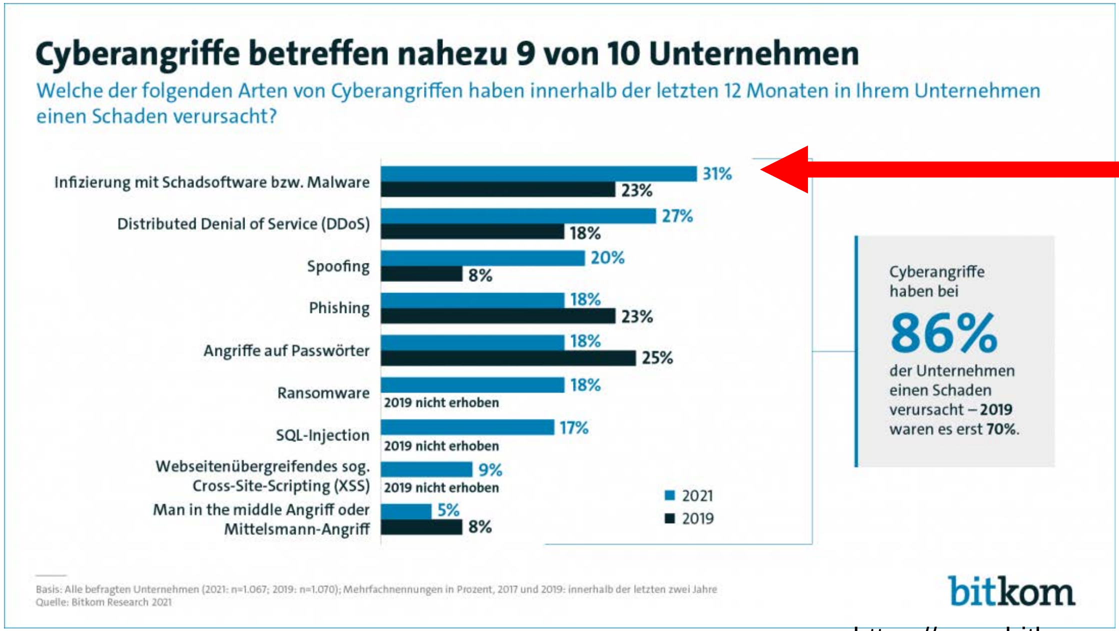
Hoch zuverlässige und sichere Software mit Ada

KI/ML Engineering

Tool Entwicklung

Cyber Kriminalität (Bitkom Studie 5.8.2021)

- Gesamtschaden von 223 Milliarden Euro /a durch Diebstahl, Spionage und Sabotage für deutsche Wirtschaft
  (2018/2019: 103 Milliarden Euro /a)
- Neun von zehn Unternehmen (88 Prozent) 2020/2021 von Angriffen betroffen
  (2018/2019: drei Viertel = 75 Prozent)



Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

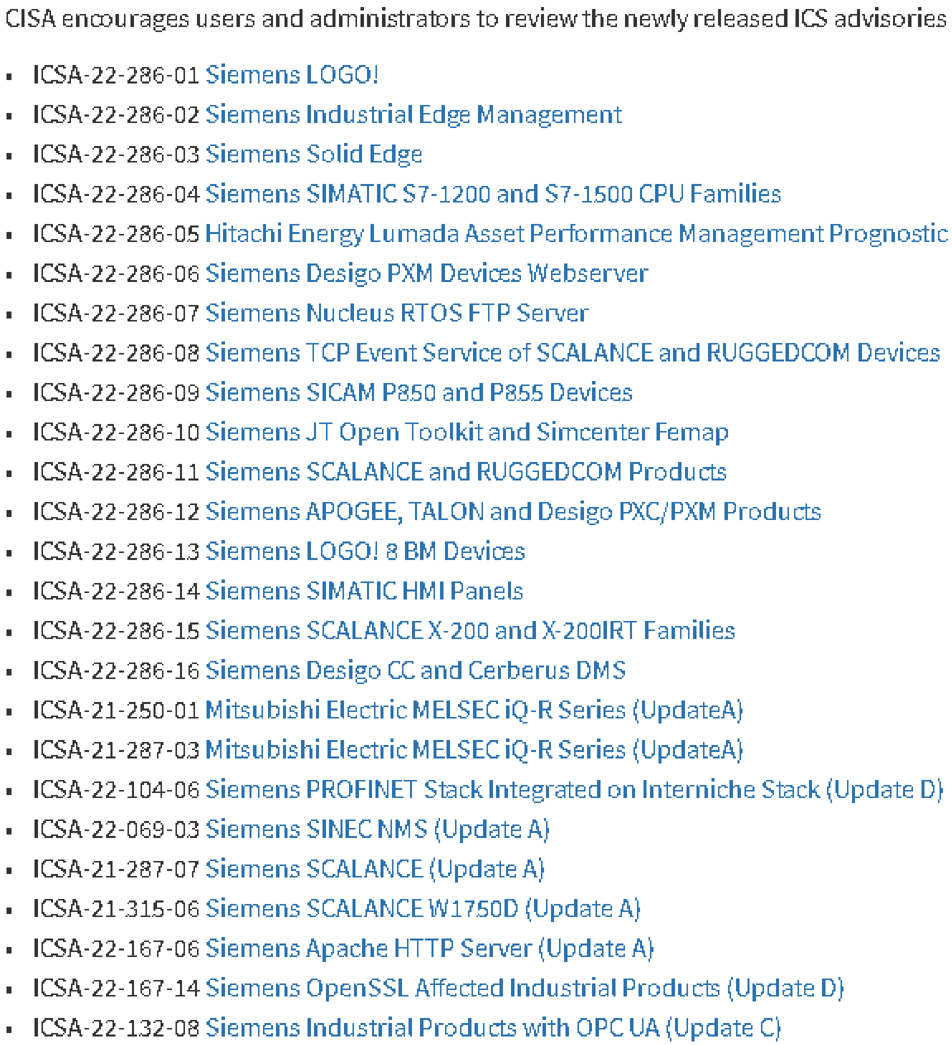
Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre
Quelle: Bitkom Research 2021

Ursache der Schwachstellen zum Eindringen:
Manipulation von Eingabedaten
→ **Vulnerabilities**

https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

CISA Releases Twenty-Five Industrial Control Systems Advisories Original release date: October 13, 2022



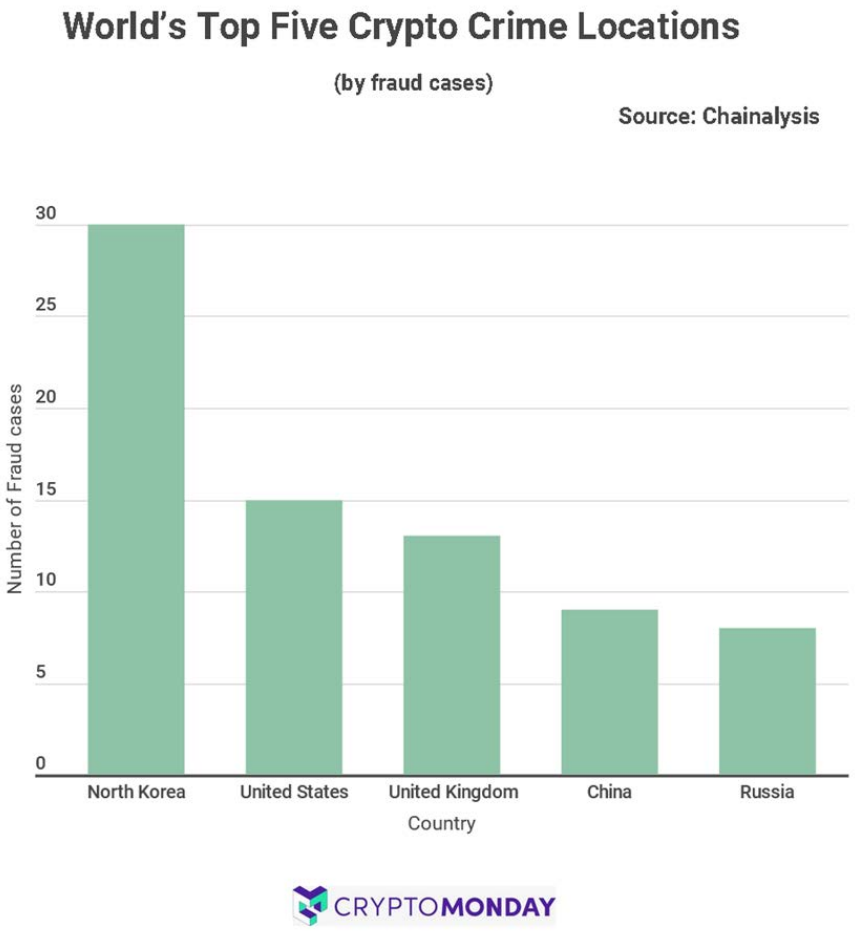
CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations:

- ICSA-22-286-01 Siemens LOGO!
- ICSA-22-286-02 Siemens Industrial Edge Management
- ICSA-22-286-03 Siemens Solid Edge
- ICSA-22-286-04 Siemens SIMATIC S7-1200 and S7-1500 CPU Families
- ICSA-22-286-05 Hitachi Energy Lumada Asset Performance Management Prognostic Model Executor Service
- ICSA-22-286-06 Siemens Desigo PXM Devices Webserver
- ICSA-22-286-07 Siemens Nucleus RTOS FTP Server
- ICSA-22-286-08 Siemens TCP Event Service of SCALANCE and RUGGEDCOM Devices
- ICSA-22-286-09 Siemens SICAM P850 and P855 Devices
- ICSA-22-286-10 Siemens JT Open Toolkit and Simcenter Femap
- ICSA-22-286-11 Siemens SCALANCE and RUGGEDCOM Products
- ICSA-22-286-12 Siemens APOGEE, TALON and Desigo PXC/PXM Products
- ICSA-22-286-13 Siemens LOGO! 8 BM Devices
- ICSA-22-286-14 Siemens SIMATIC HMI Panels
- ICSA-22-286-15 Siemens SCALANCE X-200 and X-200IRT Families
- ICSA-22-286-16 Siemens Desigo CC and Cerberus DMS
- ICSA-21-250-01 Mitsubishi Electric MELSEC iQ-R Series (UpdateA)
- ICSA-21-287-03 Mitsubishi Electric MELSEC iQ-R Series (UpdateA)
- ICSA-22-104-06 Siemens PROFINET Stack Integrated on Interniche Stack (Update D)
- ICSA-22-069-03 Siemens SINEC NMS (Update A)
- ICSA-21-287-07 Siemens SCALANCE (Update A)
- ICSA-21-315-06 Siemens SCALANCE W1750D (Update A)
- ICSA-22-167-06 Siemens Apache HTTP Server (Update A)
- ICSA-22-167-14 Siemens OpenSSL Affected Industrial Products (Update D)
- ICSA-22-132-08 Siemens Industrial Products with OPC UA (Update C)

Link: https://www.cisa.gov/uscert/ncas/current-activity/2022/10/13/cisa-releases-twenty-five-industrial-control-systems-advisories

Krypto-Diebstähle

- Nordkoreanische Hacker haben allein im Jahr 2022 über eine Milliarde US-Dollar erbeutet. Hinter den Cyberangriffen soll das nordkoreanische Regime stecken (Studie des Nachrichtenportals CryptoMonday).
- Daran hat vor allem das Hackerkollektiv "Lazarus" den größten Anteil (Jonathan Merry, CEO von CryptoMonday).
- Erst im vergangenen Monat haben die Hacker bei einem Cyberangriff auf die kalifornische Blockchain Harmony rund 100 Millionen US-Dollar erbeutet.
- Im März gelang es den Kriminellen, den größten Krypto-Raub aller Zeiten zu begehen: Nach Auskunft des US-Finanzministeriums wurden dabei rund 615 Millionen US-Dollar erbeutet.



https://cryptomonday.de/news/2022/07/28/north-korean-hackers-responsible-for-over-dollar1-billion-stolen-in-2022/

CVE / CWE Definitionen

W=Weakness=Schwachstelle
V=Vulnerability=Angreifbarkeit=angreifbare Schwachstelle

Weaknesses are errors that can lead to vulnerabilities. A software vulnerability, such as those enumerated on the Common Vulnerabilities and Exposures (CVE®) List, is a mistake in software that can be directly used by a hacker to gain access to a system or network.

CVE - Common Vulnerabilities and Exposures

CVE® Program Mission (Industriestandard zur Benennung von Sicherheitslücken in Computersystemen, https://www.cve.org/)

- Currently, there are 180.175 CVE Records accessible

- The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.
- There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program.
- Partners publish CVE Records to communicate consistent descriptions of vulnerabilities.
- Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

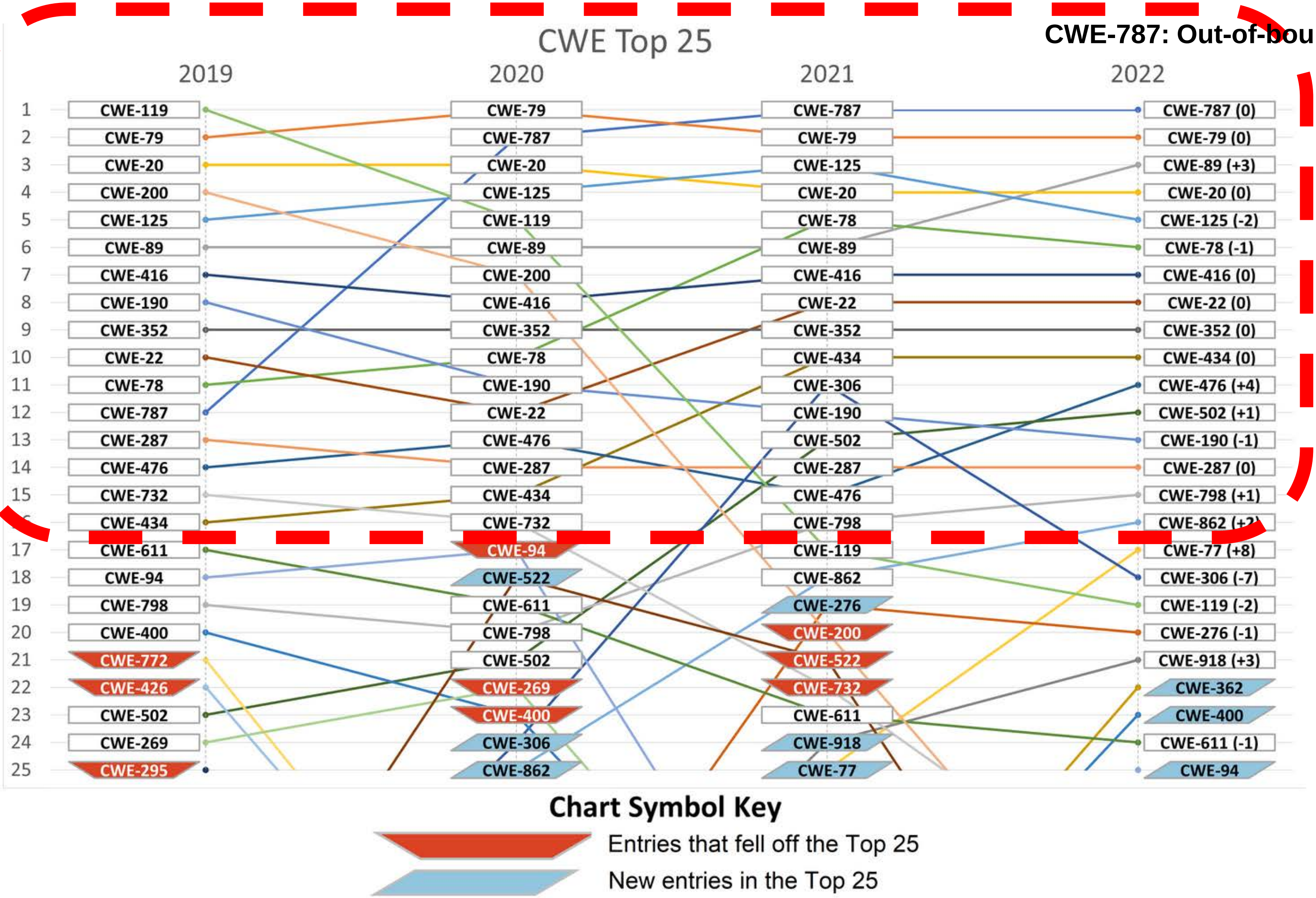
CWE – Common Weakness Enumeration

- CWE™ (community-developed list of software and hardware weakness types, https://cwe.mitre.org/index.html)
- It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

2022 CWE Top 25 Most Dangerous Software Weaknesses

- They are dangerous because they are often easy to find, exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working.
- https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html#cwe_top_25 sowie

CWE 2019 – 2022 – eine stabile (Fehler-) Welt



CWE Top 25

	2019	2020	2021	2022
1	CWE-119	CWE-79	CWE-787	CWE-787 (0)
2	CWE-79	CWE-787	CWE-79	CWE-79 (0)
3	CWE-20	CWE-20	CWE-125	CWE-89 (+3)
4	CWE-200	CWE-125	CWE-20	CWE-20 (0)
5	CWE-125	CWE-119	CWE-78	CWE-125 (-2)
6	CWE-89	CWE-89	CWE-89	CWE-78 (-1)
7	CWE-416	CWE-200	CWE-416	CWE-416 (0)
8	CWE-190	CWE-416	CWE-22	CWE-22 (0)
9	CWE-352	CWE-352	CWE-352	CWE-352 (0)
10	CWE-22	CWE-78	CWE-434	CWE-434 (0)
11	CWE-78	CWE-190	CWE-306	CWE-476 (+4)
12	CWE-787	CWE-22	CWE-190	CWE-502 (+1)
13	CWE-287	CWE-476	CWE-502	CWE-190 (-1)
14	CWE-476	CWE-287	CWE-287	CWE-287 (0)
15	CWE-732	CWE-434	CWE-476	CWE-798 (+1)
16	CWE-434	CWE-732	CWE-798	CWE-862 (+2)
17	CWE-611	CWE-94	CWE-119	CWE-77 (+8)
18	CWE-94	CWE-522	CWE-862	CWE-306 (-7)
19	CWE-798	CWE-611	CWE-276	CWE-119 (-2)
20	CWE-400	CWE-798	CWE-200	CWE-276 (-1)
21	CWE-772	CWE-502	CWE-522	CWE-918 (+3)
22	CWE-426	CWE-269	CWE-732	CWE-362
23	CWE-502	CWE-400	CWE-611	CWE-400
24	CWE-269	CWE-306	CWE-918	CWE-611 (-1)
25	CWE-295	CWE-862	CWE-77	CWE-94

Chart Symbol Key

🟥 Entries that fell off the Top 25

🟦 New entries in the Top 25

CWE-787: Out-of-bounds Write

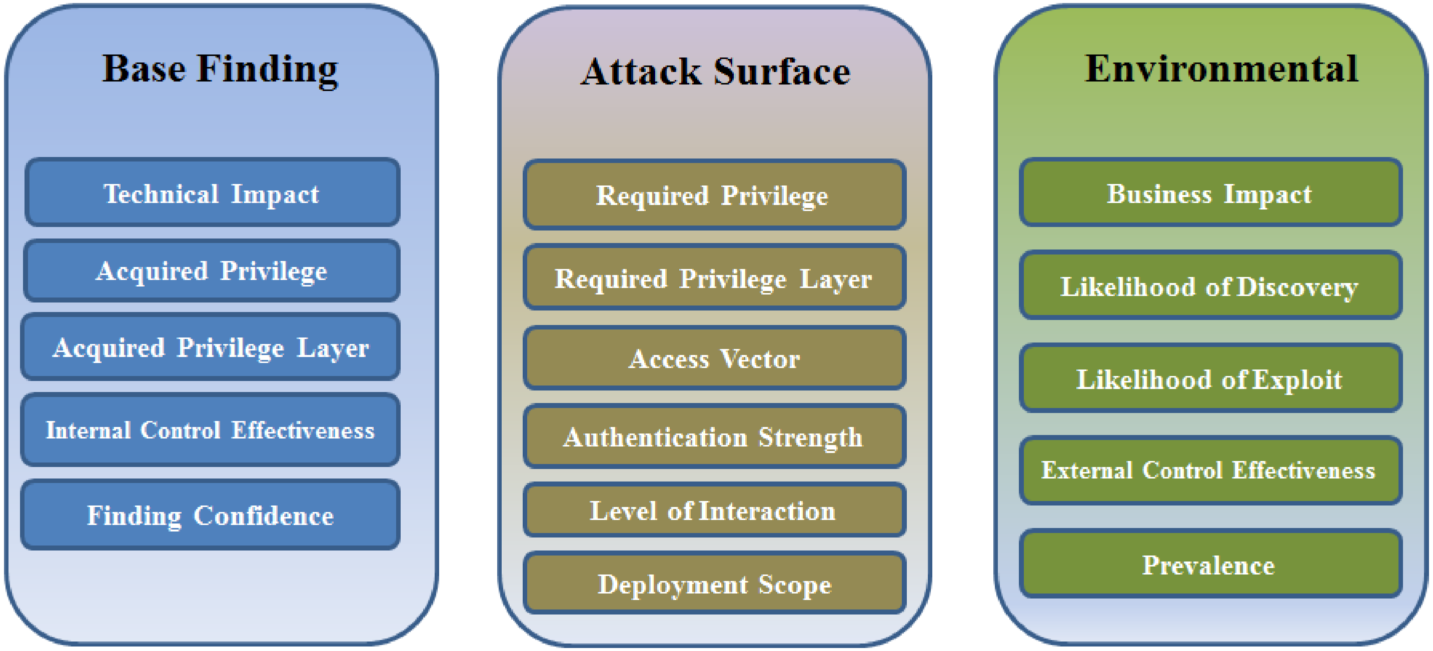
CWE-20: Improper Input Validation

CWE-125: Out-of-bounds Read

CWSS – Scoring System

Common Weakness Scoring System (CWSS™)

- CWSS is organized into three metric groups: Base Finding, Attack Surface, and Environmental (https://cwe.mitre.org/cwss/cwss_v1.0.1.html).
- Each group contains multiple metrics - also known as factors - that are used to compute a CWSS score for a weakness.

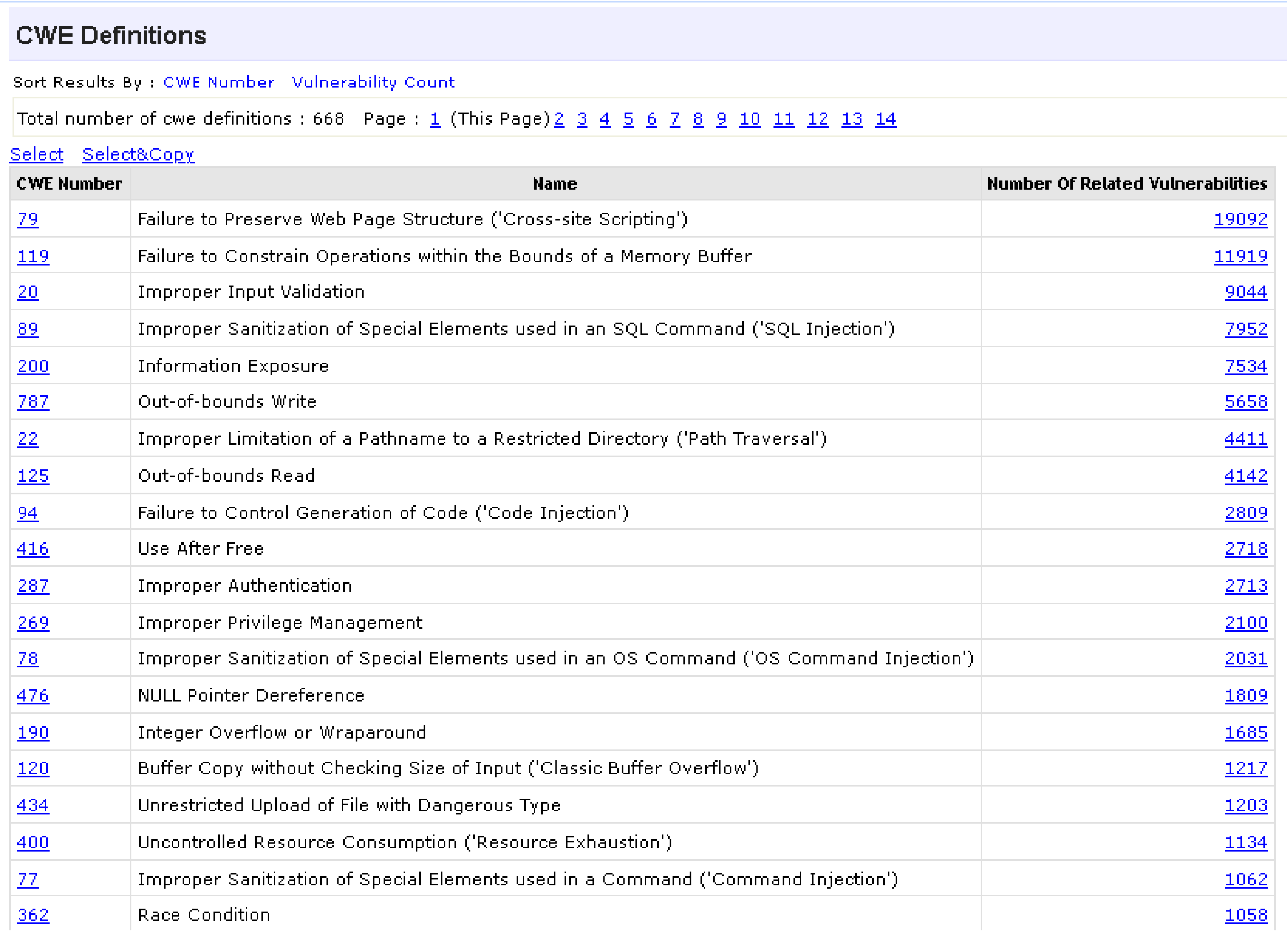


CVE Details

- Provides an easy to use web interface to CVE vulnerability data.
- You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them.
- You can view statistics about vendors, products and versions of products.
- CVE details are displayed in a single, easy to use page, see a sample here.

- CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institue of Standards and Technology.
- Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data.
- https://www.cvedetails.com/index.php

CWE nach vulnerability count



CWE Definitions

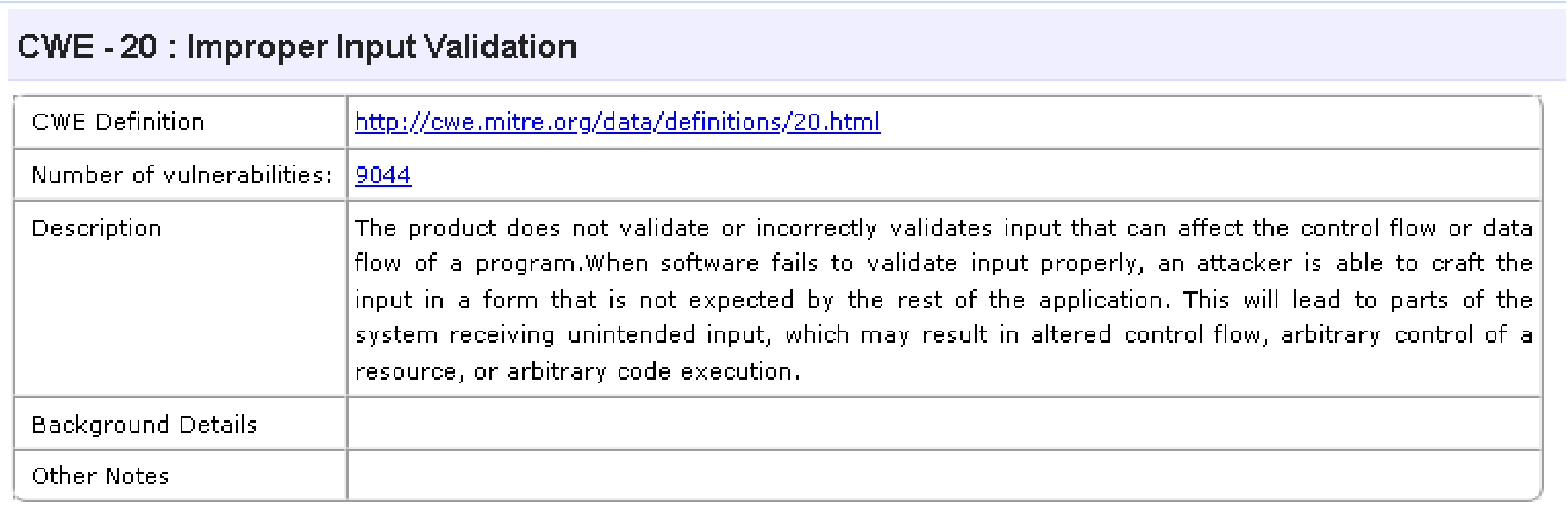
Sort Results By : CWE Number Vulnerability Count

Total number of cwe definitions : 668 Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14

Select Select&Copy

CWE Number	Name	Number Of Related Vulnerabilities
79	Failure to Preserve Web Page Structure ('Cross-site Scripting')	19092
119	Failure to Constrain Operations within the Bounds of a Memory Buffer	11919
20	Improper Input Validation	9044
89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')	7952
200	Information Exposure	7534
787	Out-of-bounds Write	5658
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	4411
125	Out-of-bounds Read	4142
94	Failure to Control Generation of Code ('Code Injection')	2809
416	Use After Free	2718
287	Improper Authentication	2713
269	Improper Privilege Management	2100
78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	2031
476	NULL Pointer Dereference	1809
190	Integer Overflow or Wraparound	1685
120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1217
434	Unrestricted Upload of File with Dangerous Type	1203
400	Uncontrolled Resource Consumption ('Resource Exhaustion')	1134
77	Improper Sanitization of Special Elements used in a Command ('Command Injection')	1062
362	Race Condition	1058

Beispiel CWE - 20



CWE - 20 : Improper Input Validation

CWE Definition	http://cwe.mitre.org/data/definitions/20.html
Number of vulnerabilities:	9044
Description	The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program.When software fails to validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.
Background Details	
Other Notes	

See https://cwe.mitre.org/data/definitions/1387.html

Zur Situation
(Momentaufnahme)

Berliner Gesamtkonferenz der Sicherheitsinstitutionen

Meldungen US-CERT

- High Score
  microsoft -- windows_server_2012
  Microsoft Windows Support Diagnostic Tool (MSDT): **Remote Code Execution Vulnerability**.
  2022-06-01. **Kritikalität: 9.3**
  Betroffen: Windows 11, 10, 8, 7, Server 2008 bis 2012
  Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190

- Medium Score
  cisco -- common_services_platform_collector
  Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC).
  Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to **insufficient validation of user-supplied input** by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to **execute arbitrary script code** in the context of the interface or access sensitive, browser-based information.
  2022-05-27. Kritikalität: 4.3
  Details: https://nvd.nist.gov/vuln/detail/CVE-2022-20666

…

- pharmacy_management_system_project -- pharmacy_management_system
  Pharmacy Management System v1.0 was discovered to contain a **remote code execution (RCE) vulnerability** via the component php_action/editProductImage.php.
  This vulnerability allows attackers to **execute arbitrary code** via a crafted image file.
  Date: 2022-05-20. Kritikalität: 7.5
  Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30887
- SSA-165073: Multiple Vulnerabilities in the Webinterface **of SICAM P850 and SICAM P855** Devices
  Publication Date: 2022-05-10. **Kritikalität: 9.8**
  Multiple vulnerabilities were identified in the webserver of SICAM P850 and SICAM P855 devices. These include unauthenticated access to web-interface functionality, missing HTTPS or impersonation as well as cross-site scripting related vulnerabilities
  Details: https://cert-portal.siemens.com/productcert/pdf/ssa-165073.pdf
- **VMware** Workspace ONE Access, Identity Manager and vRealize Automation contain an **authentication bypass vulnerability** affecting local domain users. A malicious actor with network access to the UI may be able to **obtain administrative access** without the need to authenticate.
  Kritikalität: 9.8
  Details: https://nvd.nist.gov/vuln/detail/CVE-2022-22972
- **VMware** Workspace ONE Access and Identity Manager contain a **privilege escalation vulnerability**.
  A malicious actor with local access can escalate privileges to 'root'.
  Kritikalität: 7.8
  Details: https://nvd.nist.gov/vuln/detail/CVE-2022-22973

…

- **Cisco Releases Security Updates for Enterprise NFV Infrastructure Software**
  Cisco has released security updates to address **multiple vulnerabilities** in Enterprise NFV Infrastructure Software. An attacker could exploit these vulnerabilities to **take control of an affected system**.
  Original release date: May 5, 2022

Meldungen CISA - Cybersecurity and Infrastructure Security Agency

- **Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control**.
  These vulnerabilities affect certain versions of VMware Workspace ONE Access, VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation, and vRealize Suite Lifecycle Manager.
  Exploiting these vulnerabilities permits malicious actors to trigger a server-side template injection that may result in remote code execution (RCE) (CVE-2022-22954) or escalation of privileges to root (CVE-2022-22960).
  Original release date: **May 18, 2022**
- CISA Updates Advisory on Threat Actors Chaining Unpatched VMware Vulnerabilities.
  Original release date: **June 02, 2022**
- Carrier LenelS2 HID Mercury access panels
  This advisory contains mitigations for Protection Mechanism Failure, Forced Browsing, Classic Buffer Overflow, Path Traversal, and OS Command Injection vulnerabilities in Carrier HID Mercury access panels sold by LenlS2.
  June 2, 2022
  (LenelS2 is the global leader in advanced physical security solutions, including access control, video surveillance and mobile credentialing)
- Illumina Local Run Manager
  This advisory contains mitigations for Path Traversal, Unrestricted Upload of File with Dangerous Type, Improper Access Control, and Cleartext Transmission of Sensitive Information vulnerabilities in Illumina devices using Local Run Manager software

...

- ICS Medical Advisory (ICSMA-22-151-01)
  BD Pyxis
  Successful exploitation of this vulnerability could allow an attacker to gain access to electronic protected health information (ePHI) or other sensitive information.
  Original release date: May 31, 2022. Kritikalität: 8.8

- CISA Adds 34 Known Exploited Vulnerabilities to Catalog
  CISA has added 34 new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.
  Original release date: May 25, 2022
- CISA Adds 20 Known Exploited Vulnerabilities to Catalog
  Original release date: May 24, 2022

- CISA Issues Emergency Directive and Releases Advisory Related to VMware Vulnerabilities
  CISA has issued Emergency Directive (ED) 22-03 and released a Cybersecurity Advisory (CSA) in response to active and expected exploitation of multiple vulnerabilities in the following VMware products: VMware Workspace ONE Access (Access), VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation, vRealize Suite Lifecycle Manager.
  Original release date: May 18, 2022

…

- CISA releases 27 Industrial Control Systems Advisories
  ICS-CERT released the following 27 advisories today, May 12, 2022
- Delta Electronics CNCSoft
  This advisory contains mitigations for Stack-based Buffer Overflow, and Out-of-bounds Read vulnerabilities in the Delta Electronics CNCSoft software management platform.
- Mitsubishi Electric MELSOFT iQ AppPortal
  This advisory contains mitigations for Missing Authorization, Out-of-bounds Write, NULL Pointer Dereference, Classic Buffer Overflow, HTTP Request Smuggling, and Infinite Loop vulnerabilities in Mitsubishi Electric MELSOFT iQ AppPortal products.
- Inkscape in Industrial Products
  This advisory contains mitigations for Out-of-bounds Read, Access of Uninitialized Pointer, and Out-of-bounds Write vulnerabilities in the Inkscape open-source graphics editor.
- Cambium Networks cnMaestro
  This advisory contains mitigations for OS Command Injection, SQL Injection, Path Traversal, and Use of Potentially Dangerous Function vulnerabilities in the Cambium Networks cnMaestro network management system.
- Siemens Industrial PCs and CNC devices
  This advisory contains mitigations for Improper Input Validation, Improper Authentication, Improper Isolation of Shared Resources on System-on-a-Chip, and Improper Privilege Management vulnerabilities in Siemens Industrial PCs and CNC devices.

…

- Siemens SIMATIC WinCC
  This advisory contains mitigations for an Insecure Default Initialization of Resource vulnerability in SIMATIC PCS and WinCC industrial products.
- Siemens SICAM P850 and SICAM P855
  This advisory contains mitigations for Improper Neutralization of Parameter/Argument Delimiters, Cleartext Transmission of Sensitive Information, Cross-site Scripting, Missing Authentication for Critical Function, Authentication Bypass by Capture-replay, and Improper Authentication vulnerabilities in Siemens SICAM P850 and SICAM P855 electrical variable measuring devices.
- Siemens Industrial Products with OPC UA
  This advisory contains mitigations for a Null Pointer Dereference vulnerability in Siemens industrial products using the OPC UA AMSOC stack.
- Siemens JT2GO and Teamcenter Visualization
  This advisory contains mitigations for Infinite Loop, Null Pointer Dereference, Integer Overflow to Buffer Overflow, Double Free, and Access of Uninitialized Pointer vulnerabilities in Siemens JT2GO, Teamcenter Visualization products.
- Siemens Desigo PXC and DXR Devices
  This advisory contains mitigations for an Uncaught Exception vulnerability in the Siemens Desigo DXR and PXC controllers.

…

- Siemens SIMATIC CP 44x-1 RNA
  This advisory contains mitigations for an Uncontrolled Resource Consumption vulnerability in the Siemens SIMATIC CP 44x-1 RNA.
- Siemens Industrial Products
  This advisory contains mitigations for an Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in the OPC Foundation Local Discovery Server in multiple Siemens industrial products.
- Siemens Industrial Devices using libcurl
  This advisory contains mitigations for a Use After Free vulnerability in Siemens Industrial Devices using libcurl.
- Siemens Simcenter Femap
  This advisory contains mitigations for an Out-of-bounds Write vulnerability in the Siemens Simcenter Femap advanced simulation application.
- Siemens OpenV2G
  This advisory contains mitigations for a Classic Buffer Overflow vulnerability in the open-source implementation of the ISO/IEC vehicle-to-grid communication interface (V2G CI) standard.
- Siemens Teamcenter
  This advisory contains mitigations for Stack-based Buffer Overflow, and Improper Restriction of XML External Entity Reference vulnerabilities in the Siemens Teamcenter product lifecycle management software.

…

- Siemens OpenSSL Vulnerabilities in Industrial Products (Update A)
  This updated advisory is a follow-up to the original advisory titled ICSA-22-104-05 Siemens OpenSSL Vulnerabilities in Industrial Products that was published April 14, 2022, on the ICS webpage at cisa.gov/ics. This advisory contains mitigations for a NULL Pointer Dereference vulnerability in the Siemens OpenSSL.
- Mitsubishi Electric GT25-WLAN (Update A)
  This updated advisory is a follow-up to the original advisory titled ICSA-22-102-04 Mitsubishi Electric GT25-WLAN that was published April 12, 2022, on the ICS webpage on cisa.gov/ics. This advisory contains mitigations for Improper Removal of Sensitive Information Before Storage or Transfer, Inadequate Encryption Strength, Missing Authentication for Critical Function, Injection, and Improper Input Validation vulnerabilities in Mitsubishi Electric GT25-WLAN wireless communication units.
- Siemens SIMATIC WinCC and PCS (Update B)
  This updated advisory is a follow-up to the advisory update titled ICSA-22-041-02 Siemens SIMATIC WinCC and PCS (Update A) that was published April 14, 2022, to the ICS webpage on cisa.gov/ics. This advisory contains mitigations for Exposure of Sensitive Information to an Unauthorized Actor, and Insertion of Sensitive Information into Externally-Accessible File or Directory vulnerabilities in Siemens SIMATIC WinCC and PCS industrial automation products.
- Siemens SIMATIC WinCC (Update D)
  This updated advisory is a follow-up to the advisory update titled ICSA-21-315-03 Siemens SIMATIC WinCC (Update C) that was published April 14, 2022, to the ICS webpage on cisa.gov/ics. This advisory contains mitigations for a Path Traversal, and Insertion of Sensitive Information into Log File vulnerabilities in Siemens SIMATIC WinCC, a SCADA HMI system.

…

- Siemens Nucleus RTOS-based APOGEE and TALON (Update C)
  This updated advisory is a follow-up to the advisory update titled ICSA-21-315-07 Siemens Nucleus RTOS-based APOGEE and TALON Products (Update B) that was published April 14, 2022, on the ICS webpage at cisa.gov/ics. This advisory contains mitigations for several vulnerabilities in Siemens Nucleus RTOS-based APOGEE and TALON direct digital control (DDC) devices.
- Siemens VxWorks-based Industrial Products (Update B)
  This updated advisory is a follow-up to the advisory update titled ICSA-21-194-12 Siemens Wind River VxWorks-based Industrial Products (Update A) that was published April 14, 2022, on the ICS webpage on cisa.gov/ics. This advisory includes mitigations for a Heap-based Buffer Overflow in Siemens Industrial Products incorporating the Wind River VxWorks product.
- Siemens SIMATIC RFID (Update B)
  This updated advisory is a follow-up to the advisory update titled ICSA-21-159-13 Siemens SIMATIC RFID Readers (Update A) that was published April 14, 2022, on the ICS webpage on cisa.gov/ics. This advisory contains mitigations for an Uncontrolled Resource Consumption vulnerability in Siemens Simatic RFID industrial hardware systems.
- Siemens SIMOTICS, Desigo, APOGEE, and TALON (Update D)
  This updated advisory is a follow-up to the advisory update titled ICSA-20-105-06 Siemens SIMOTICS, Desigo, APOGEE, and TALON (Update C) that was published April 14, 2021, on the ICS webpage at cisa.gov/ics. This advisory contains mitigations for a Business Logic Errors vulnerability in Siemens SIMOTICS, Desigo, APOGEE, and TALON products.

…

- Siemens SCALANCE and SIMATIC (Update H)
  This updated advisory is a follow-up to the advisory update titled ICSA-20-105-07 Siemens SCALANCE & SIMATIC (Update G) that was published April 14, 2022, to the ICS webpage on cisa.gov/ics. This advisory contains mitigations for a Resource Exhaustion vulnerability in Siemens SCALANCE and SIMATIC products.
- Siemens TIA Portal (Update D)
  This updated advisory is a follow-up to the advisory update titled ICSA-20-014-05 Siemens TIA Portal (Update C) that was published December 16, 2021, on the ICS webpage at cisa.gov/ics. This advisory contains mitigations for a Path Traversal vulnerability in the Siemens TIA Portal engineering framework.
- Siemens Industrial Products (Update R)
  This updated advisory is a follow-up to the advisory update titled ICSA-19-253-04 Siemens Industrial Products (Update Q) published on April 14, 2022, to the ICS webpage on cisa.gov/ics. This updated advisory includes mitigations for Integer Excessive Data Query Operations in a Large Data Table, Integer Overflow or Wraparound, and Resource Exhaustion vulnerabilities reported in Siemens' industrial products.

CISA releases 30 Industrial Control Systems Advisories

- ICS-CERT released the **following 30 advisories today**, July 14, 2022. Click on the links below for more detailed information on these Industrial Control Systems vulnerabilities.
- Link zu den Meldungen
- **CISA Vulnerability Summary for the Week of October 10, 2022** https://www.cisa.gov/uscert/ncas/bulletins/sb22-290

NIST

- NIST Cybersecurity and Privacy Program
  New EO Guidance for **Cybersecurity Supply Chain Risk Management**
  NIST has released a revision of Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST Special Publication 800-161 Revision 1).

- NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. Our activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

- https://www.nist.gov/cybersecurity

Zu den Ursachen

Berliner Gesamtkonferenz der Sicherheitsinstitutionen

Common Weakness Enumeration - CWE

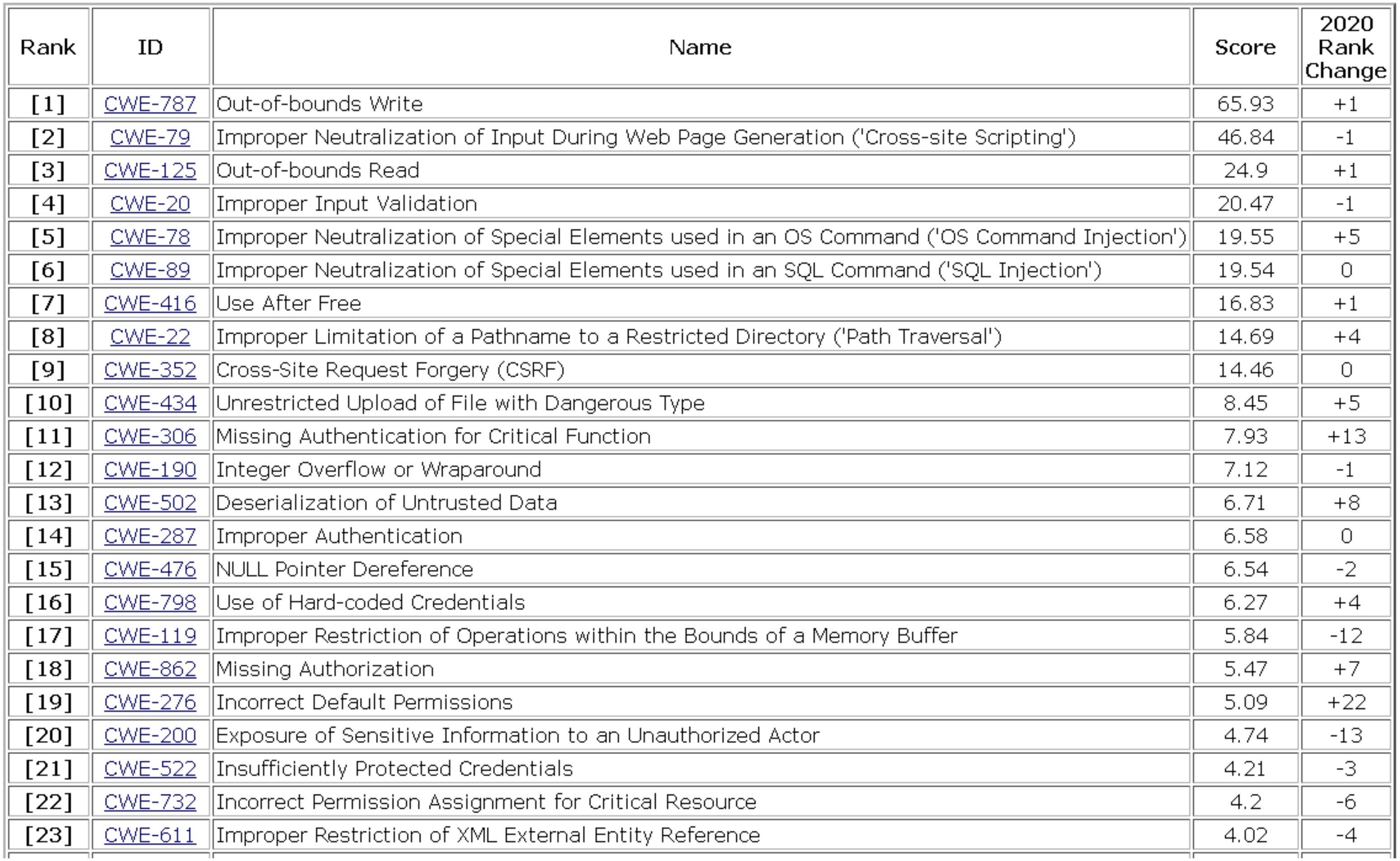
- Listed by vulnerability count

CWE Number	Name	Number Of Related Vulnerabilities
79	Failure to Preserve Web Page Structure ('Cross-site Scripting')	18666
119	Failure to Constrain Operations within the Bounds of a Memory Buffer	11926
20	Improper Input Validation	9036
89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')	7617
200	Information Exposure	7519
787	Out-of-bounds Write	5451
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	4337
125	Out-of-bounds Read	4067
94	Failure to Control Generation of Code ('Code Injection')	2817
287	Improper Authentication	2769
416	Use After Free	2670
269	Improper Privilege Management	2308
78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	1966
476	NULL Pointer Dereference	1775
190	Integer Overflow or Wraparound	1659
400	Uncontrolled Resource Consumption ('Resource Exhaustion')	1175
120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1170
434	Unrestricted Upload of File with Dangerous Type	1161
77	Improper Sanitization of Special Elements used in a Command ('Command Injection')	1057

https://www.cvedetails.com/cwe-definitions/1/orderbyvulnerabilities.html?order=2&trc=668&sha=0427874cc45423ccb6974ee25935fbfceac76fcb

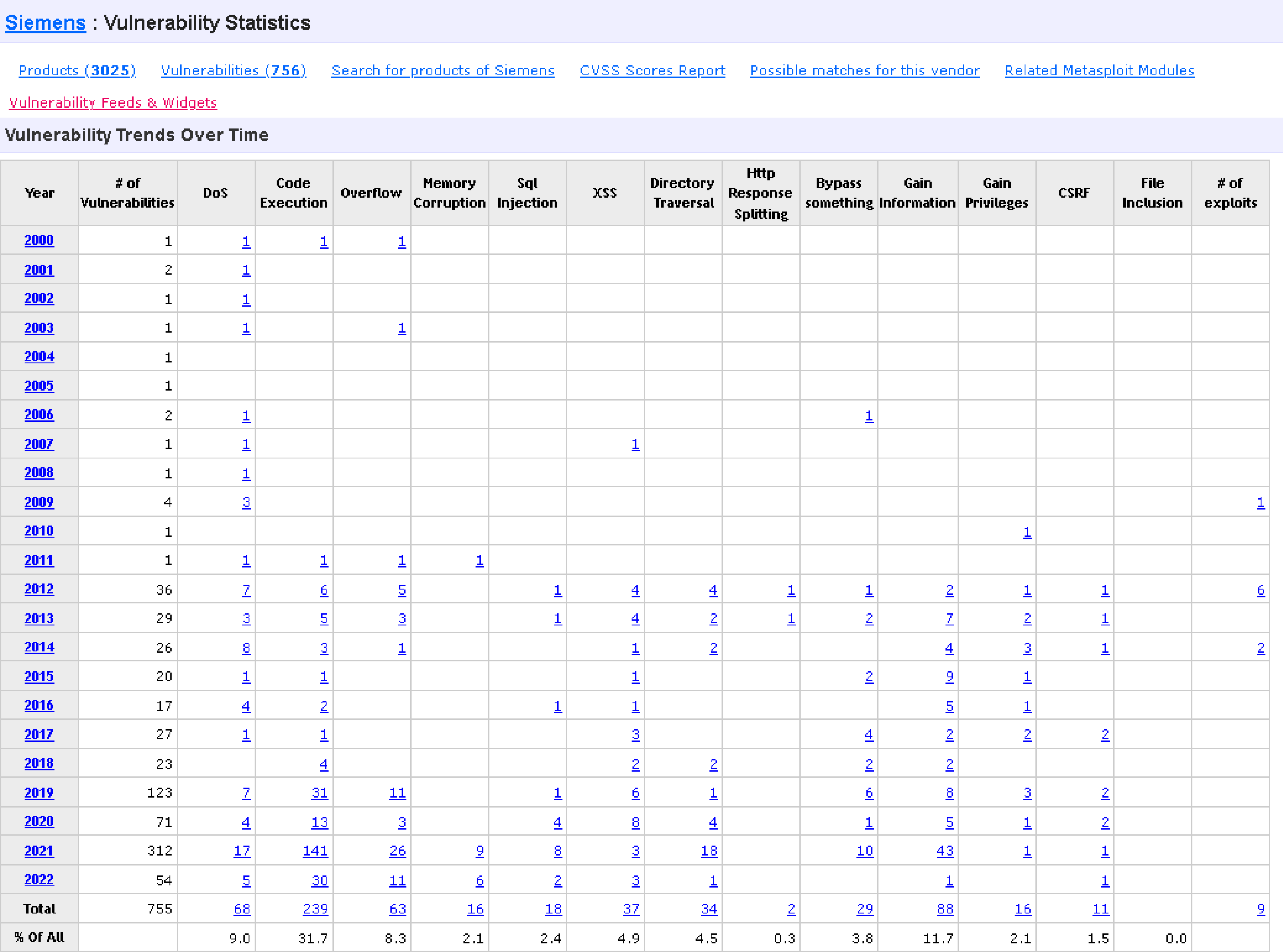
...

- 2021 CWE Top 25 Most Dangerous Software Weaknesses



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
[13]	CWE-502	Deserialization of Untrusted Data	6.71	+8
[14]	CWE-287	Improper Authentication	6.58	0
[15]	CWE-476	NULL Pointer Dereference	6.54	-2
[16]	CWE-798	Use of Hard-coded Credentials	6.27	+4
[17]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	5.84	-12
[18]	CWE-862	Missing Authorization	5.47	+7
[19]	CWE-276	Incorrect Default Permissions	5.09	+22
[20]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	4.74	-13
[21]	CWE-522	Insufficiently Protected Credentials	4.21	-3
[22]	CWE-732	Incorrect Permission Assignment for Critical Resource	4.2	-6
[23]	CWE-611	Improper Restriction of XML External Entity Reference	4.02	-4

… by Vendors



Siemens : Vulnerability Statistics

Products (3025) Vulnerabilities (756) Search for products of Siemens CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2000	1	1	1	1											
2001	2	1													
2002	1	1													
2003	1	1		1											
2004	1														
2005	1														
2006	2	1								1					
2007	1	1					1								
2008	1	1													
2009	4	3													1
2010	1											1			
2011	1	1	1	1	1										
2012	36	7	6	5		1	4	4	1	1	2	1	1		6
2013	29	3	5	3		1	4	2	1	2	7	2	1		
2014	26	8	3	1			1	2			4	3	1		2
2015	20	1	1				1			2	9	1			
2016	17	4	2			1	1				5	1			
2017	27	1	1				3			4	2	2	2		
2018	23		4				2	2		2	2				
2019	123	7	31	11		1	6	1		6	8	3	2		
2020	71	4	13	3		4	8	4		1	5	1	2		
2021	312	17	141	26	9	8	3	18		10	43	1	1		
2022	54	5	30	11	6	2	3	1			1		1		
Total	755	68	239	63	16	18	37	34	2	29	88	16	11		9
% Of All		9.0	31.7	8.3	2.1	2.4	4.9	4.5	0.3	3.8	11.7	2.1	1.5	0.0	

Ursachen Vulnerabilities? Ihre Meinung!

- Remote Code Execution Vulnerability
- insufficient validation of user-supplied input
- Improper Input Validation
- Classic Buffer Overflow
- Stack-based Buffer Overflow
- Out-of-bounds Write
- Out-of-bounds Read
- Null Pointer Dereference
- Integer Overflow to Buffer Overflow
- Double Free
- Use After Free

- authentication bypass vulnerability
- privilege escalation vulnerability
- multiple vulnerabilities
- Improper Authentication

- Cleartext Transmission of Sensitive Information

Zur sinnvollen Vorgehensweise (Ursachenbeseitigung)

Aspekte für Security

- Design Architektur Gesamtsystem
  - Security by Design

- Benutzerverwaltung
  - Strenge Authentifizierung
  - Minimale Rechtevergabe
  - Nur absolut notwendige Software einsetzen

- Kommunikationsprotokolle und Verschlüsselung
  - Identifikation des Kommunikationspartners sichern (Hash ID)
  - Zuverlässigkeit des Protokolls sicher stellen
  - Verschlüsselung der Übertragung
  - Zeitliche Gültigkeit des Schlüssels nach Risiko

- 99% aller Prozessoren sind Embedded Systems
  - Effiziente, aber sichere Software

…

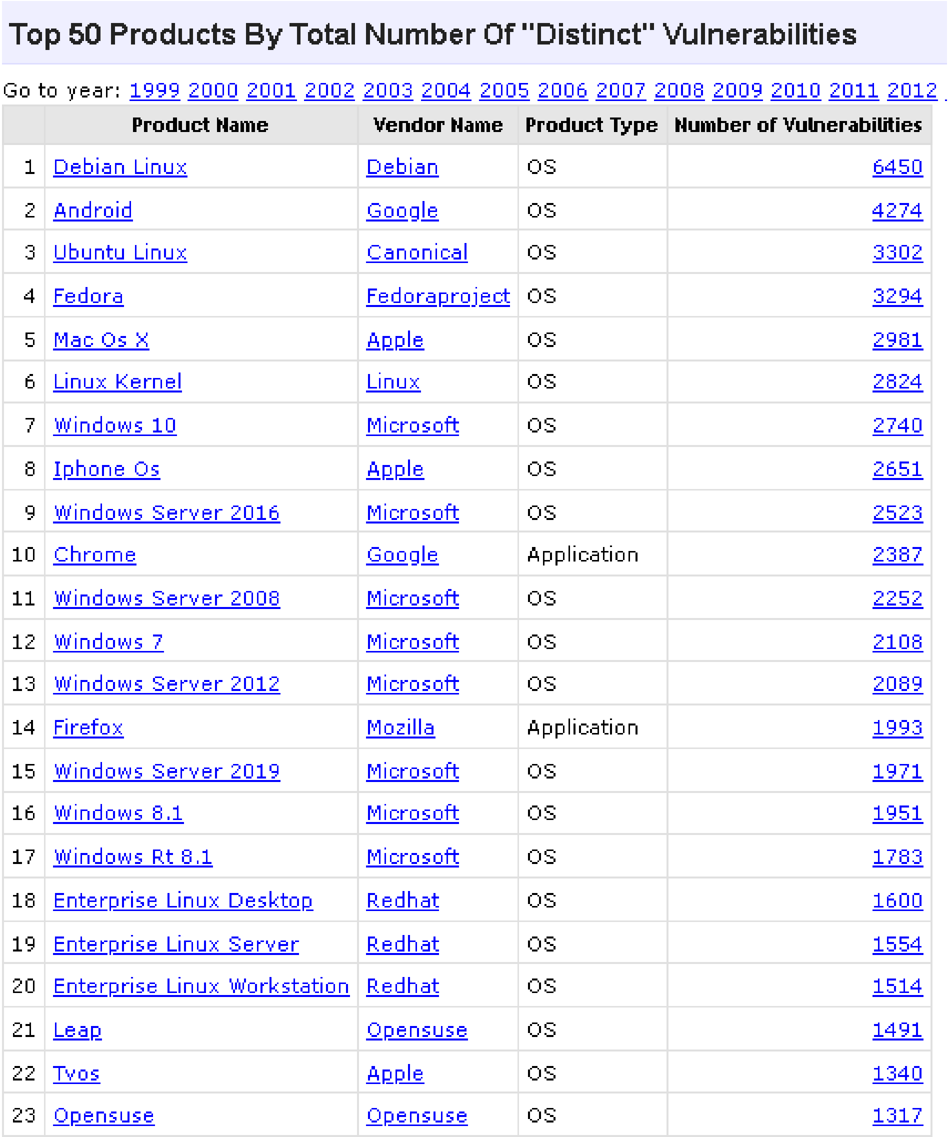
- Implementierung
  - Code durch automatische Analyse auf Einhaltung prüfen lassen (formale Verifikation durch SPARK)
  - sichere Algorithmen verwenden bzw. updaten
  - sichere Programmiersprache verwenden (kein C/C++, kein Java)
  - jedes Eingabedatum syntaktisch und semantisch prüfen
  - siehe Vorgabe Seacord und NE153
- Cloud & Micro Cloud Services (Rechtefluss und –prüfung)
  - Rechtevergabe über Serviceanfragen auf Micro Services abbilden/prüfen
- Agiles Vorgehen und die Nanosicht
  - agiles Vorgehen kennt keine Architektursicht des Gesamtsystems (vom Prinzip ← Story Card)
  - Security ist eine Architektureigenschaft
  - Security als Feature von Beginn an berücksichtigen

...

- Betriebssysteme?

- Deutscher L4 Kernel
  - in USA zertifiziert!
  - In D nicht vorhanden

    → Abhängigkeiten statt Diversifikation bzw. eigene Kompetenz



Top 50 Products By Total Number Of "Distinct" Vulnerabilities

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 .

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	6450
2	Android	Google	OS	4274
3	Ubuntu Linux	Canonical	OS	3302
4	Fedora	Fedoraproject	OS	3294
5	Mac Os X	Apple	OS	2981
6	Linux Kernel	Linux	OS	2824
7	Windows 10	Microsoft	OS	2740
8	Iphone Os	Apple	OS	2651
9	Windows Server 2016	Microsoft	OS	2523
10	Chrome	Google	Application	2387
11	Windows Server 2008	Microsoft	OS	2252
12	Windows 7	Microsoft	OS	2108
13	Windows Server 2012	Microsoft	OS	2089
14	Firefox	Mozilla	Application	1993
15	Windows Server 2019	Microsoft	OS	1971
16	Windows 8.1	Microsoft	OS	1951
17	Windows Rt 8.1	Microsoft	OS	1783
18	Enterprise Linux Desktop	Redhat	OS	1600
19	Enterprise Linux Server	Redhat	OS	1554
20	Enterprise Linux Workstation	Redhat	OS	1514
21	Leap	Opensuse	OS	1491
22	Tvos	Apple	OS	1340
23	Opensuse	Opensuse	OS	1317

Zu Akteuren und Aktivitäten international

Berliner Gesamtkonferenz der Sicherheitsinstitutionen

Institutionen

- USA
  NIST, US CERT, ICS CERT, Homeland
  → konzertierte Aktionen
  Reports und Standards
  hohe Aktivität
- Deutschland
  BSI, VDI, VDE, ITG, ZVEI, …
  → jeder für sich und keiner gesamt (Führungsebene?)
- Niederlande
  NSA als nationale Behörde

- Adressierung von Problemen der Programmiersprache
  ISO / IEC Arbeitsgruppe mit Report → Report nicht offen zugänglich
  allgemein nicht berücksichtigt

  Aber: C/C++ Standards ohne Indexprüfung etc., undefined behavior

Secure Coding in C and C++ (Robert C. Seacord)

Software Engineering Institute, Carnegie Mellon University

- … To address the growing number of both vulnerabilities and incidents, it is increasingly apparent that the problem must be attacked at the source by working to prevent the introduction of software vulnerabilities during software development and ongoing maintenance.
- Analysis of existing vulnerabilities indicates that a relatively small number of root causes accounts for the majority of vulnerabilities. …
- However, even the best designs can lead to insecure programs if developers are unaware of the many security pitfalls inherent in C and C++ programming.
- … Root causes of software vulnerabilities, such as buffer overflows, integer type range errors, and invalid format strings, are identified and explained where applicable.
- Strategies for securely implementing functional capabilities are described in each chapter, as well as techniques for discovering vulnerabilities in existing code.

Robert C. Seacord is (was) the Secure Coding Technical Manager in **the CERT Program** of Carnegie Mellon's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania. Now at Woven Planet Holdings, Inc., a subsidiary of the Toyota Motor Corporation, formerly the Toyota Research Institute – Advanced Development (TRI–AD). (https://en.wikipedia.org/wiki/Robert_C._Seacord)

Akteure in Deutschland

- Politik
  zeigt sich ohne Verständnis der Problematik
- BMI
  lässt sich beraten, Flughöhe extrem
- BSI
  hat Doppelfunktion, soll schützen und gleichzeitig einbrechen
  keine echte Vernetzung und keine tiefe Durchdringung
- BAM, PtB, DIN, TÜV
  glauben an Normung als Grundlage von Security
  sehen ein Businessmodell (DIN)
- Universitäten
  bilden nicht in nachhaltiger und sicherer Softwareentwicklung aus
  methodische Schwachstellen
  entwickeln lieber komplexe und nicht anwendbare Modelle
  kein Handwerkszeug für Industrie
  agile Vorgehensweise sieht kein Gesamtbild
- Industrie
  konzentrieren sich auf „nice features“ wie Autonomes Fahren (geht nicht wegen Kontextkomplexität)
  mehr Marketing und Sprüche statt Handlung
  Schwachstellen setzen sich sukzessive fort

Forschungseinrichtungen und Universitäten
Laut Verfassungsschutz greifen mutmaßlich staatliche chinesische Hackergruppen gezielt **wissenschaftliche Einrichtungen** in Deutschland an. Statt Millionen zu investieren, können **Forschungsergebnisse** so auch einfach gestohlen werden. Deutsche Hochschulen sind ein leichtes Ziel – und oft bemerkenswert sorglos: Etliche kooperieren mit chinesischen Unis, an denen staatliche Hacker trainiert werden.

Angriff auf TU Berlin, April 2021: Rund 400.000 Euro kostete die Reparatur der geschädigten IT-Systeme.

Chinesische APT Gruppen („Advanced Persistent Threat“)

https://correctiv.org/aktuelles/wirtschaft/2022/07/21/offene-tueren-fuer-cyberangriffe-deutsche-hochschulen-forschen-mit-chinesischen-hacker-fabriken/

Zitate „Athene Vortrag SIT, Darmstadt 21.7.2022“

- Recht-Wenig Erfahrung in Deutschland
  - International sehr viel Erfahrung, insb. in den USA
  - Kompetenzen über Behörden verteilt
  - Wenig praktische Erfahrung
  - Cyberabwehr braucht schnelle, halbautomatisierte, internationale Abstimmung
  - …
  - Kryptographie muss kompromisslos stark sein, ohne Hintertüren
  - Schwachstellen sollen schnellstmöglich geschlossen werden

Resümee

Lessons learned –
PISEA Ergebnis in Safety und IT-Security

(PISEA – a Programme for International Science and Engineering Assessment)

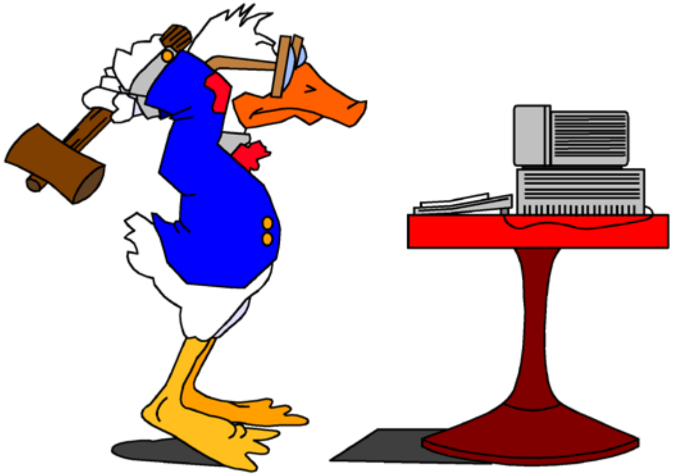
- Sichere Architekturen (Cloud?, Agile Development?)
- Sichere Zugänge
- Sichere Kommunikation
- Sichere Implementierung!

- Sicherheits-Bewusstsein (Entwicklung, Management, Politik, Gesellschaft)
- Sicheres Vorgehen
- Sicherheits-Vorgaben

- Kriminelle wollen im Moment nur Geld ohne Schaden
- Staaten sind schon kritischer (massive Manipulation, Wirtschaftsspionage)
- Terroristen sind (noch) inkompetent

Cyber Security Kosten: Konsequenzen ← hohe Eintrittswahrscheinlichkeit
*hoher Schaden
*hohe Ignoranz
*Unterschätzung der Angreifer
*Implementierungsschwachstellen
*???

Fragen?



https://www.pngwave.com/png-clip-art-ohqtt

h.keller@ci-tec.de
hubert.keller@dr-hbkeller.de