



Gastvortrag an der Uni Regensburg

Schwachstellenmanagement

Ein Beispiel der Maschinenfabrik Reinhausen für Produkte im KRITIS-Umfeld

16.01.2025 Dr. Hubert Feyrer



Dr. Hubert Feyrer



- + Cyber Security-Experte bei der Maschinenfabrik Reinhausen
- + 10 Jahre CISO bei Volkswagen (VW Group Services, VW Sachsen)
- + Studium in technischer Informatik der FH Regensburg
- + Promotion in Informationswissenschaften der Uni Regensburg
- + Dozent Open Source & Systemadministration in USA & Deutschland
- + Systembetreuer, Hard- und Softwareentwickler, IT-Leiter
- + Erster Vortrag beim Chaos Communications Congress vor 20 Jahren
- + Entwickler NetBSD & Mitgründer pkgsrc
- + IPv6 Pionier

Schwachstellenmanagement

Agenda

- + Über die Maschinenfabrik Reinhausen GmbH
- + Anforderungen im KRITIS-Umfeld
- + Übersicht, Hintergrund / Auslöser: log4j
- + Architektur
 - Software Component Analysis
 - SBOM – Software Bill of Materials
 - Beispiel: MR-SBOM
- + Identifizierung und Bewertung von Schwachstellen
 - Von der Komponente zur Schwachstelle
 - Automatisierung im MR-CERT
 - Security Advisories
 - Prozess & Kennzahlen
- + Ausblick: Automatisierung CSAF, SBOM
- + Praktische Übungen



Über die Maschinenfabrik Reinhausen GmbH



Auf einen Blick

Familienunternehmen seit

1868

in der fünften Generation
in Familieneigentum

Wirtschaftlich gesund

730

Mio. Euro Umsatz in 2022
Höchstes Rating (AAA)

Mitarbeiter

3.800

61 Nationalitäten
an 55 Standorten



Weltmarktführer

50%

des weltweiten Stroms
fließt durch unsere Produkte

Langlebigkeit

80%

aller Produkte noch in Betrieb,
der älteste OILTAP seit 1950

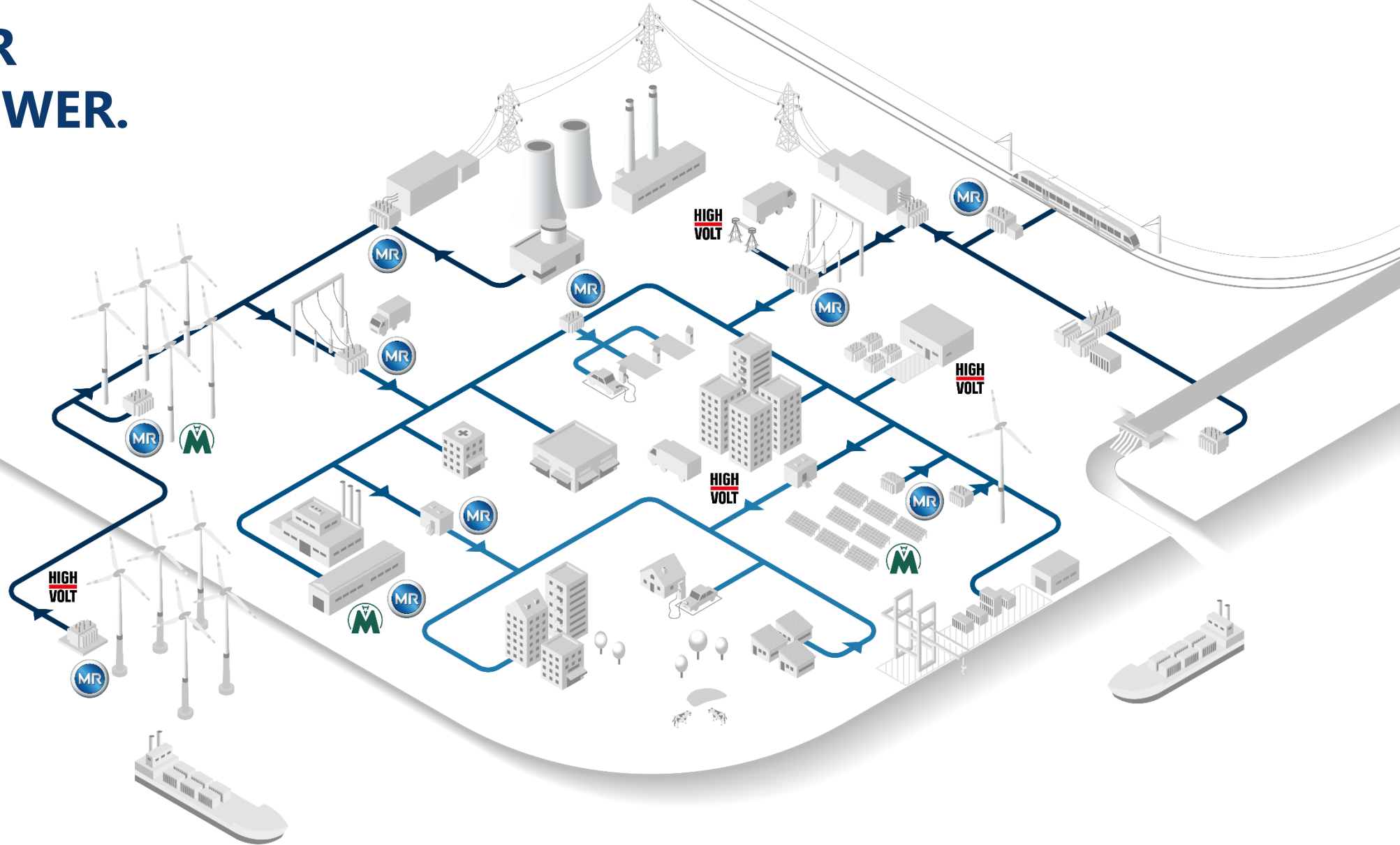
Präsent in aller Welt

8.000

Kunden
in 185 Ländern

🏭 Fabrik 📍 Büro x/x Tochtergesellschaften/Standorte

THE POWER BEHIND POWER.





Anerkannt und ausgezeichnet



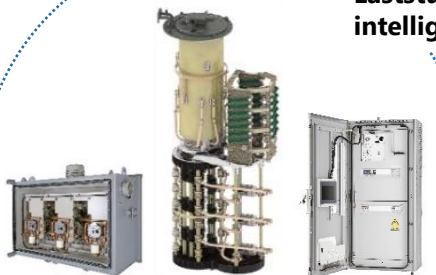




Lösungen für Lastfluss und Spannungsqualität



Transformator-Zubehör



Laststufenschalter & intelligente Antriebe



Regeltechnik für Verteiltransformatoren



Dienstleistungen im Umspannwerk



Sensorik, Automatisierung, Digitalisierung


OEM & Systemintegratoren

Netzbetreiber

Lasten & Einspeiser



Hochspannungs-Isolatoren



Hochspannungs-prüftechnik

HIGH VOLT



Power Quality Lösungen



Leistungselektronische Systeme & Komponenten



Drosseln Mittel- & Niederspannung



Anforderungen im KRITIS-Umfeld

+ Rechtlich: unterschiedlich je nach Land:

- BRD: IT-Sicherheitsgesetz + BSI
- EU: CRA + ENISA
- USA: NERC-CIP + CISA
- Beste gemeinsame Abdeckung: ISO 27001

+ Heißt:

- Schwachstellen im Produkt suchen und fixen
- Melden - Behörden, Kunden (je nach Gesetzeslage und Betroffenheit)

+ Abgrenzung:

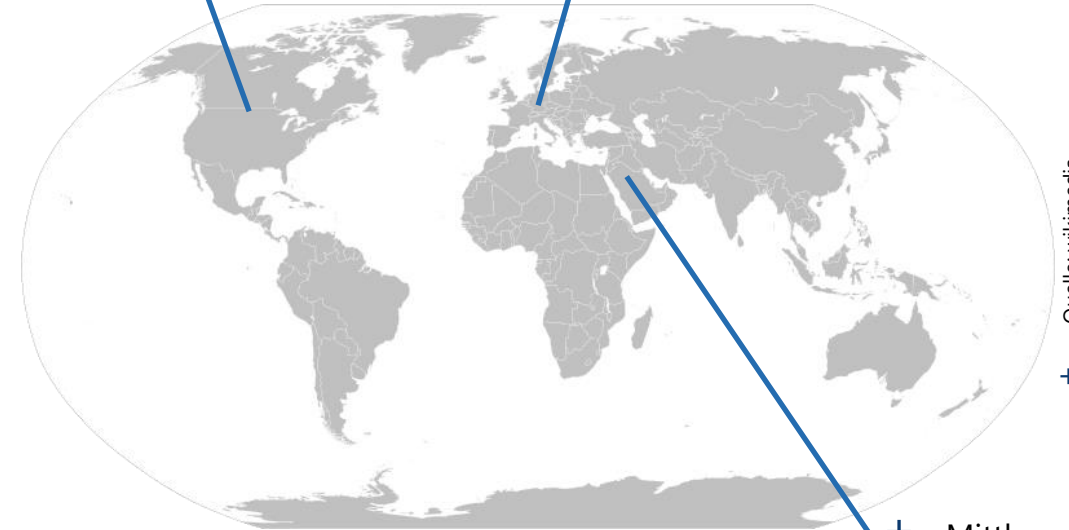
- Hier Fokus (nur) auf Produkte für das KRITIS-Umfeld
- Allgemeines Schwachstellenmanagement in KRITIS Betreiber-Umgebungen nicht im Fokus
 - > Scannen, statische/dynamische Analysen, Patchmanagement, SIEM, etc.

+ Nordamerika:

- NERC-CIP
- IEEE 1686
- ISO 27001
- NIST SP 800 Reihe

+ Europa / DACH:

- BDEW Whitepaper
- ISO 27001
- IEC 62443
- EU: NIS-2
- EU: Cyber Resilience Act
- IEC 62351



Quelle: wikimedia

+

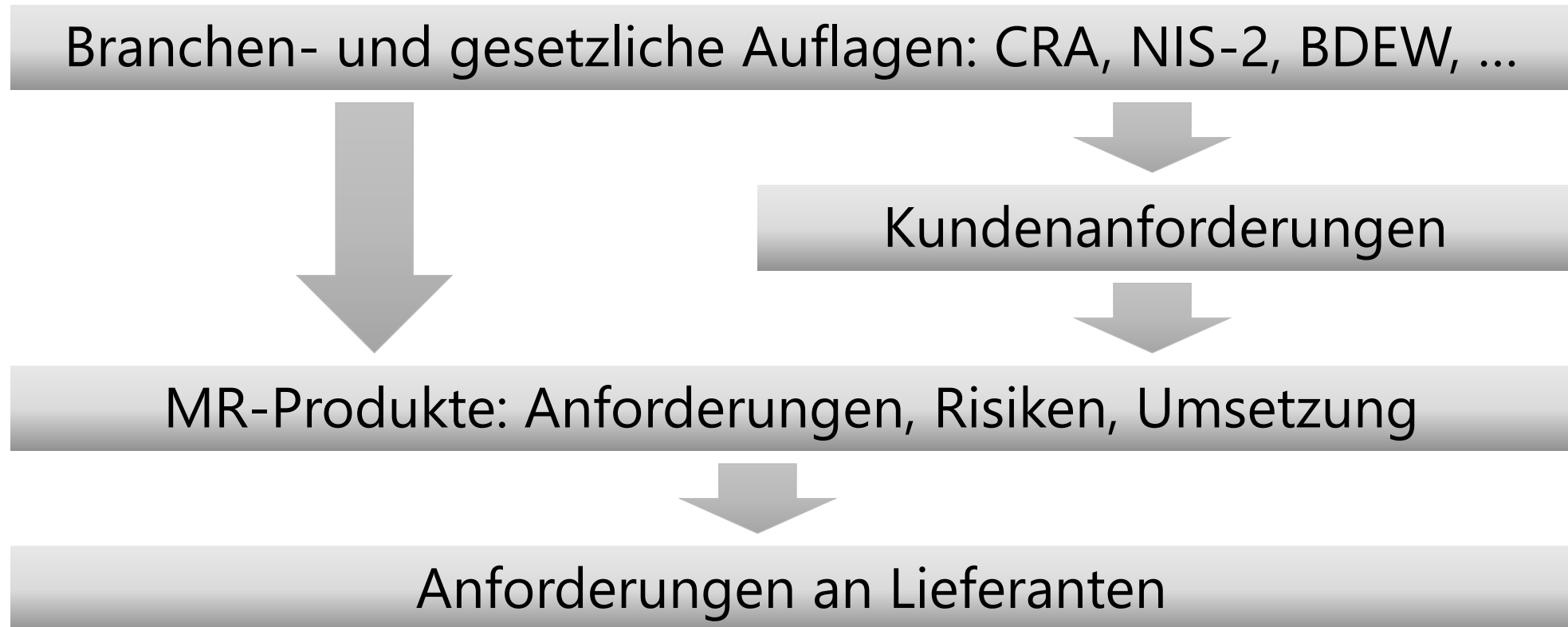
+ Mittlerer Osten

- IEEE C37.240

+ ABER: sehr viele kundenindividuellen Standards / Anforderungen!!

+ Siehe auch: <http://gridstandardsmap.com/>

Governance: Anforderungen & Betroffenheit



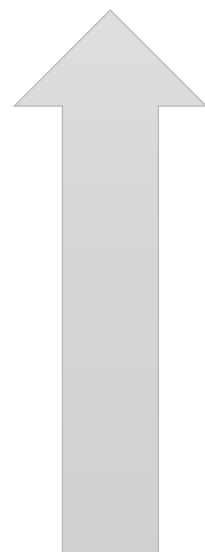
Schwachstellenmanagement



Schwachstellenmanagement Übersicht



- | Inventar und
- | Informationen über Schwachstellen
- | einholen & bewerten

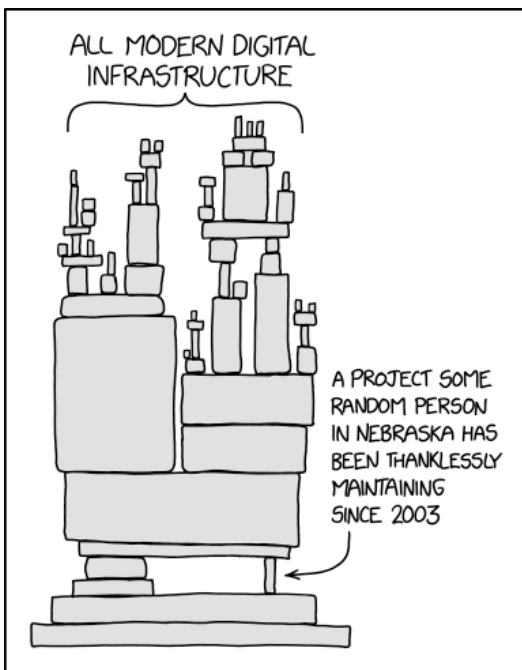


- | Schwachstellen kommunizieren (Security Advisories)
- | Produkt (Software) Updates

Schwachstellenmanagement log4j



+ Hintergrund / Auslöser: log4j

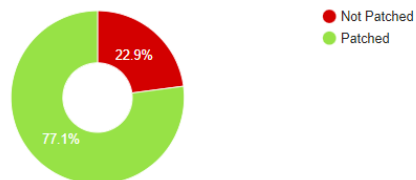


List of vendors and software affected by the Apache Log4J vulnerability (CVE-2021-44228)

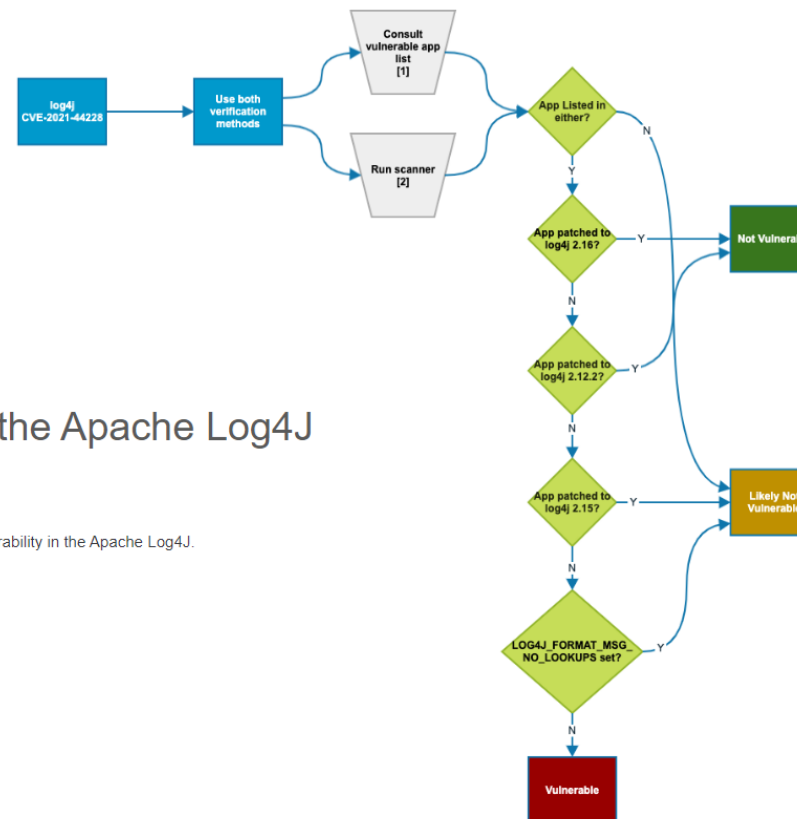
On this page we display a list of vendors and their software affected by the code injection vulnerability in the Apache Log4J. This page is being updated in real time as soon as we issue the corresponding security bulletin.

Updated: 14 days ago

Patch availability statistics by software



| | | | | |
|-----|----------------------------|--|------------|--------------|
| 282 | VMware, Inc | VMware Workspace One Access Connector | ⊗ | SB2021121424 |
| 283 | VMware, Inc | vRealize Business for Cloud | ⊗ | SB2021121425 |
| 284 | VMware, Inc | Integrated OpenStack | ⊗ | SB2021121426 |
| 285 | Wowza Media Systems | Wowza Streaming Engine | ⊗ | SB2021121427 |
| 286 | Yellowfin | Yellowfin | ⊙ | SB2021121715 |
| 287 | Zoho Corporation | Zoho ManageEngine EventLog Analyzer | ⊙ | SB2021122706 |
| 288 | ZyXEL Communications Corp. | NetAtlas Element Management System (EMS) | ⊗ | SB2021121720 |
| | | 72 | 277 | |



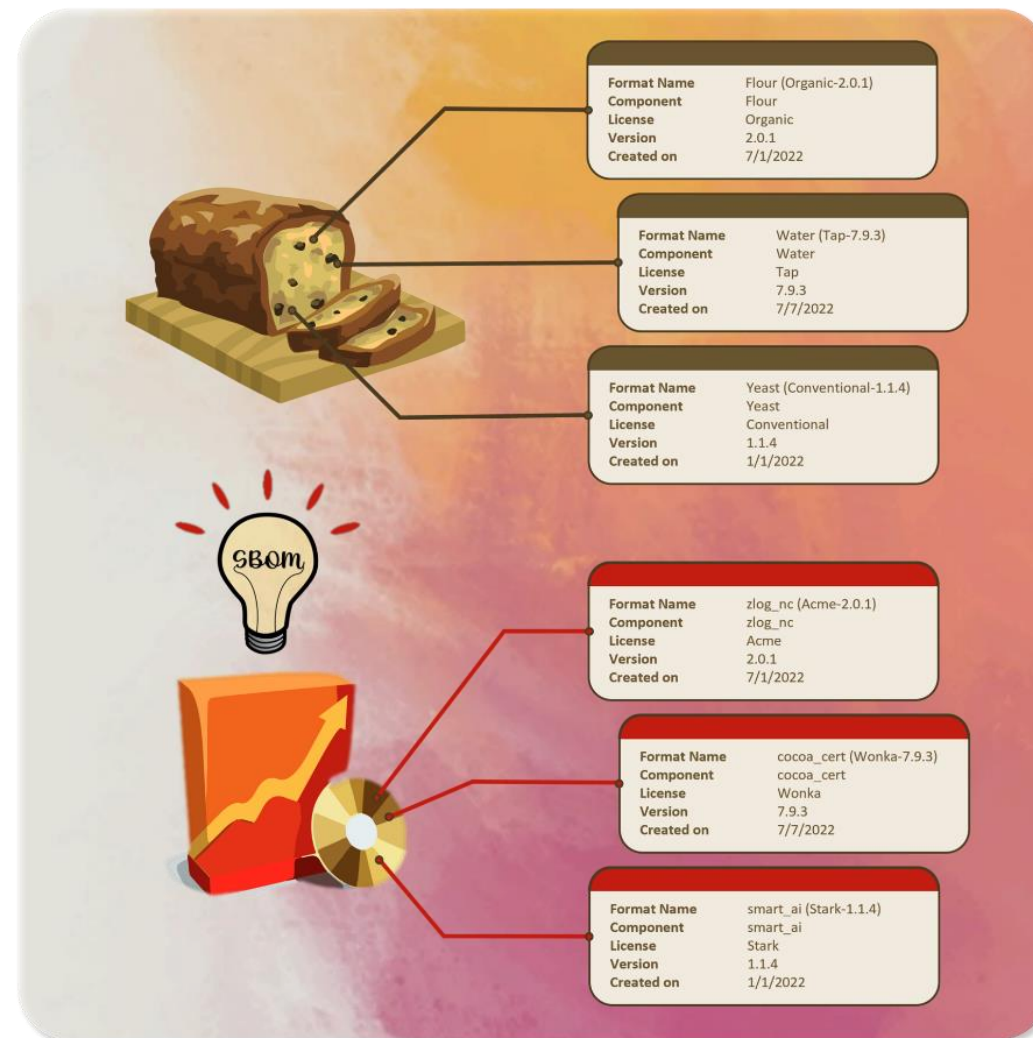
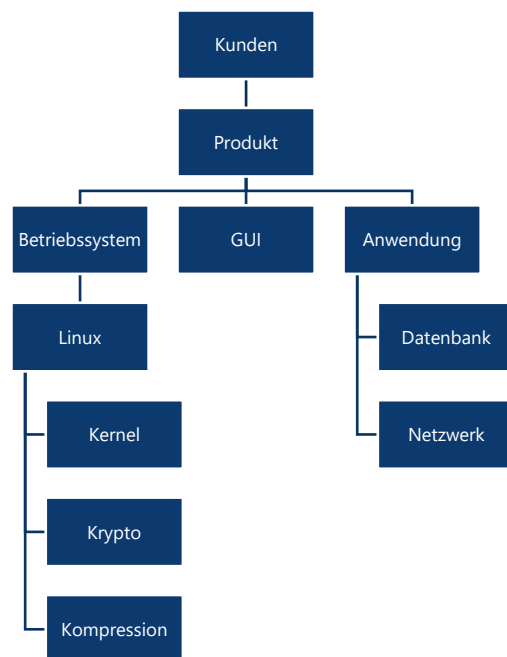
Quellen: <https://xkcd.com/2347/>
<https://www.cybersecurity-help.cz/reports/ApacheLog4J.php>
<https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>
<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Schwachstellenmanagement Architektur



- + Architektur:
- + SBOM – Software Bill of Materials
- + Software-Komponenten Up- und Downstream

+ Beispiel:



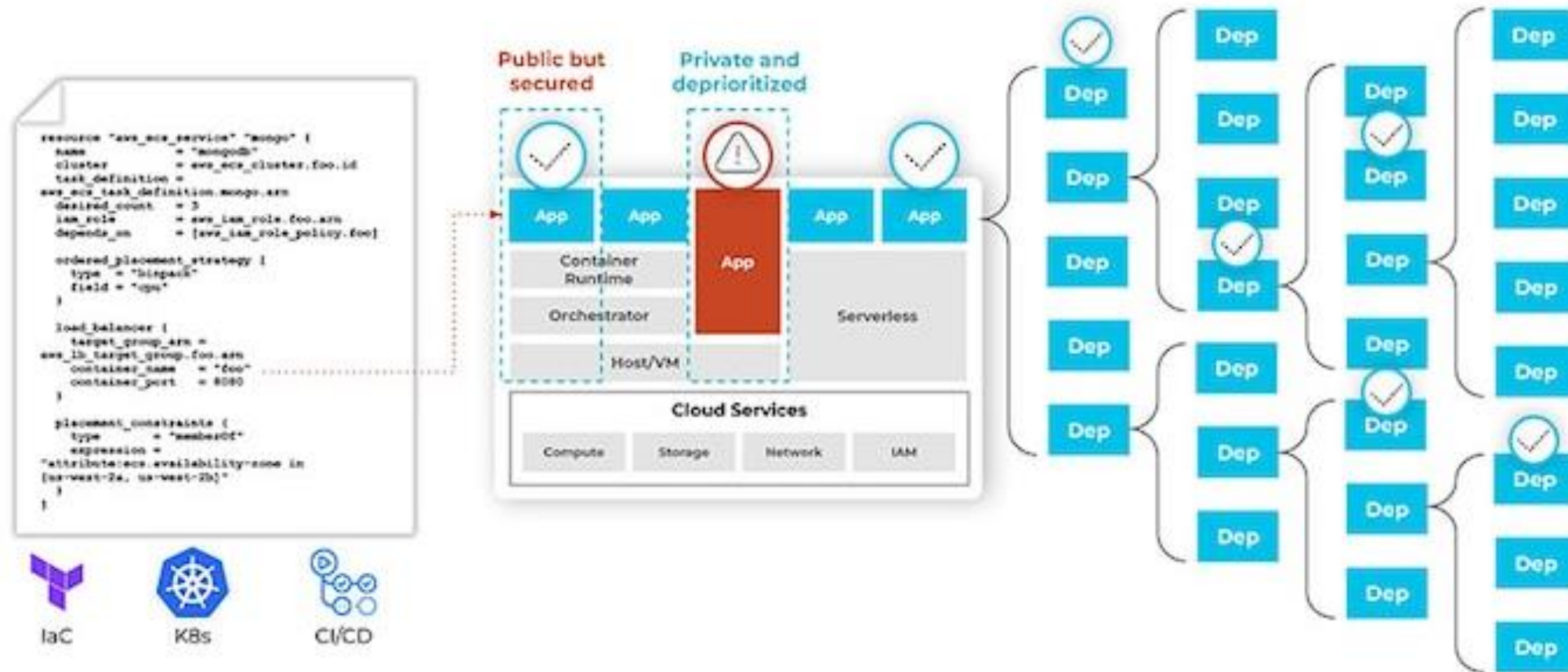
Quellen:

https://www.splunk.com/en_us/blog/industries/harmonizing-the-federal-effort-on-automating-software-bill-of-materials.html

Schwachstellenmanagement

Identifizierung von Schwachstellen

+ SCA – Software Component Analysis – Software: z.B. Black Duck, snyk, mend

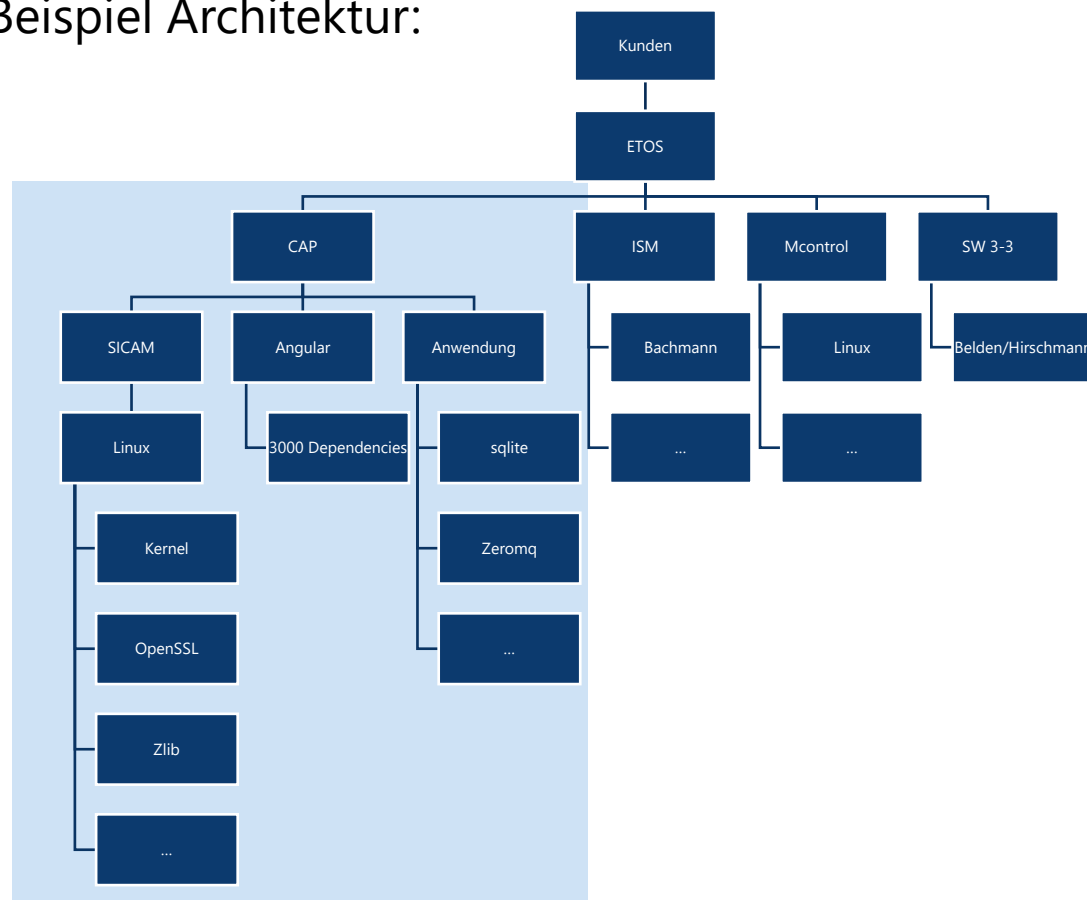


Schwachstellenmanagement

Beispiel - Architektur & SBOM



+ Beispiel Architektur:



```
*CAP.json - Editor
Datei Bearbeiten Format Ansicht Hilfe
{
  "name": "CAP",
  "version": "1.8",
  "component_name": "ETOSv1",
  "cpes": [
    "cpe:2.3:o:alpinelinux:alpine_linux:17.42",
    "cpe:2.3:a:openbsd:openssh:21.7:p1",
    "cpe:2.3:a:tinymce:tinymce:3.6.3",
    "cpe:2.3:a:sqlite:sqlite:3.28.0",
    "cpe:2.3:a:openssl:openssl:1.1.1k",
    "cpe:2.3:a:tencent:rapidjson:1.1.0",
    "cpe:2.3:a:haxx:curl:7.66.0",
    "cpe:2.3:a:libzip:libzip:1.5.2",
    "cpe:2.3:a:xmlsoft:libxml2:2.9.9",
    "cpe:2.3:a:oneidentity:syslog-ng:3.19.1",
    "cpe:2.3:a:busybox:busybox:1.30.1",
    "cpe:2.3:a:nghttp2:nghttp2:1.39.2",
    "cpe:2.3:a:musl-libc:musl:1.1.21",
    "cpe:2.3:a:pcre:pcre:8.44",
    "cpe:2.3:a:libffi:libffi:3.2.1",
    "cpe:2.3:a:gnome:glib:2.60.4",
  ],
  "environment": {
    "C": "M",
    "I": "H",
    "A": "M"
  }
}
```

Beispiel MR-SBOM mit CPES

Schwachstellenmanagement

Identifizierung von Komponenten

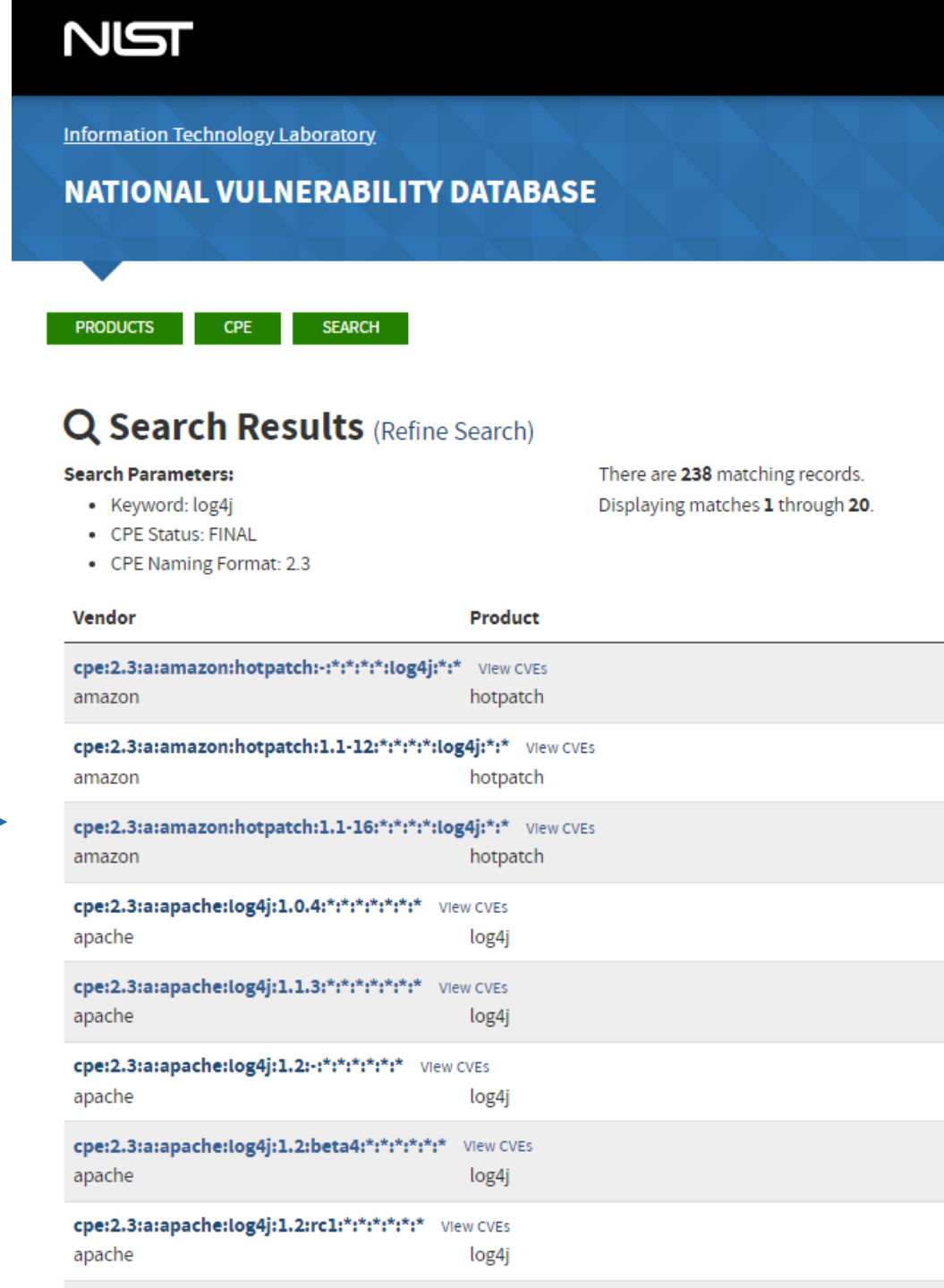
+ CPE - Common Platform Enumeration:

- Eindeutige Identifizierung von Komponenten
- Teile: Hersteller, Produktname, Produktversion (etc.)
- CPE Verzeichnis wird vom NIST unterhalten
- Herausforderung: Eindeutigkeit – z.B. bei Re-Branding, Firmen-Aufkäufen und –Umbenennungen

+ Beispiel:

Alternativen:

- PURL: Package URLs, primär node.js Umfeld, kein Mapping zu CPEs, CVEs
- SWID: ISO/IEC 19770-2:2015, nur Theorie



The screenshot shows the NIST National Vulnerability Database (NVD) search results for the keyword 'log4j'. The page header includes the NIST logo and the text 'Information Technology Laboratory' and 'NATIONAL VULNERABILITY DATABASE'. Below the header are navigation buttons for 'PRODUCTS', 'CPE', and 'SEARCH'. The search results section is titled 'Search Results (Refine Search)' and shows 'Search Parameters: Keyword: log4j, CPE Status: FINAL, CPE Naming Format: 2.3'. It also indicates 'There are 238 matching records. Displaying matches 1 through 20.' The results are presented in a table with columns for 'Vendor' and 'Product'. The first six results are listed below.

| Vendor | Product |
|--|---------------------------------------|
| cpe:2.3:a:amazon:hotpatch:-:*:*:*:log4j:*:* amazon | View CVEs hotpatch |
| cpe:2.3:a:amazon:hotpatch:1.1-12:*:*:*:log4j:*:* amazon | View CVEs hotpatch |
| cpe:2.3:a:amazon:hotpatch:1.1-16:*:*:*:log4j:*:* amazon | View CVEs hotpatch |
| cpe:2.3:a:apache:log4j:1.0.4:*:*:*:*:* apache | View CVEs log4j |
| cpe:2.3:a:apache:log4j:1.1.3:*:*:*:*:* apache | View CVEs log4j |
| cpe:2.3:a:apache:log4j:1.2:*:*:*:*:* apache | View CVEs log4j |

Schwachstellenmanagement Identifizierung von Schwachstellen



+ CVE - Common Vulnerability Enumeration:



VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions. Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type: Basic Advanced

CVSS Metrics: Version 3.x Version 2 All

Published Date Range: // / // /

Last Modified Date Range: // / // /

Contains HyperLinks: CISA Known Exploited Vulnerabilities US-CERT Technical Alerts US-CERT Vulnerability Notes OVAL Queries

Search [Reset]

Results Type: Overview Statistics

Keyword Search:

Exact Match:

CVE Identifier:

Category (CWE): Any.....

CPE: Begin typing your keyword to find the CPE. [Reset CPE Info]

Applicability Statements CPE Names

Vendor:

Product:

CVE-2021-44228 Detail

Current Description

Apache Log4j 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

[View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 10.0 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Configuration 3 (hide)

cpe:2.3:a:siemens:captial:*:*:*:*:*

[Show Matching CPE\(s\)](#)

Up to (excluding)
2019.1

cpe:2.3:a:siemens:captial:2019.1:*:*:*:*

[Show Matching CPE\(s\)](#)

- Quellen: <https://nvd.nist.gov/vuln/search>
- <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

Schwachstellenmanagement

Bewertung von Schwachstellen

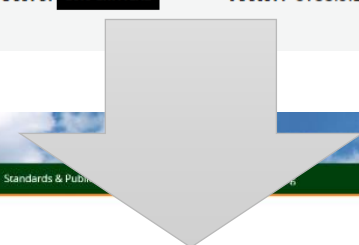


+ CVSS – Common Vulnerability Scoring System:

Severity **CVSS Version 3.x** CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score: 10.0 CRITICAL** **Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H**



Vector String - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Temporal Score **10.0 (Critical)**

Exploit Code Maturity (E)
 Not Defined (X) Unproven (U) Proof-of-Concept (P) Functional (F) High (H)

Remediation Level (RL)
 Not Defined (X) Official Fix (O) Temporary Fix (T) Workaround (W) Unavailable (U)

Report Confidence (RC)
 Not Defined (X) Unknown (U) Reasonable (R) Confirmed (C)

Environmental Score **10.0 (Critical)**

Confidentiality Requirement (CR)
 Not Defined (X) Low (L) Medium (M) High (H)

Integrity Requirement (IR)
 Not Defined (X) Low (L) Medium (M) High (H)

Availability Requirement (AR)
 Not Defined (X) Low (L) Medium (M) High (H)

Modified Attack Vector (MAV)
 Not Defined (X) Network Adjacent Network Local Physical

Modified Attack Complexity (MAC)
 Not Defined (X) Low High

Modified Privileges Required (MPR)
 Not Defined (X) None Low High

Modified User Interaction (MUI)
 Not Defined (X) None Required

Modified Scope (MS)
 Not Defined (X) Unchanged Changed

Modified Confidentiality (MC)
 Not Defined (X) None Low High

Modified Integrity (MI)
 Not Defined (X) None Low High

Modified Availability (MA)
 Not Defined (X) None Low High

About FIRST - Membership - Initiatives - Standards & Publications

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- CVSS v3.1 Documentation & Resources
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score **10.0 (Critical)**

Attack Vector (AV)
 Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)
 Low (L) High (H)

Privileges Required (PR)
 None (N) Low (L) High (H)

User Interaction (UI)
 None (N) Required (R)

Scope (S)
 Unchanged (U) Changed (C)

Confidentiality (C)
 None (N) Low (L) High (H)

Integrity (I)
 None (N) Low (L) High (H)

Availability (A)
 None (N) Low (L) High (H)

Quellen: <https://nvd.nist.gov/vuln/search>
<https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H>

Schwachstellenmanagement Automatisierung MR-CERT

+ MR-CERT CVE Server, Email & Jira:

CVE notification - Found 6 new CVEs

CVE_noreply@reinhausen.com
An [redacted] Mi 6:22

Nachricht übersetzen in: Deutsch | Nie übersetzen aus: Englisch | [Übersetzungseinstellungen](#)

CVE-2022-45884 [redacted] **MEDIUM (6.1)**
[https://reinhausen.atlassian.net/\[redacted\]](https://reinhausen.atlassian.net/[redacted])
An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c has a use-after-free, related to dvb_register_device dynamically allocating fops. Found in: linux_kernel, Version: 4.14.59

CVE-2022-45919 [redacted] **MEDIUM (6.1)**
[https://reinhausen.atlassian.net/\[redacted\]](https://reinhausen.atlassian.net/[redacted])
An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free can occur is there is a disconnect after an open, because of the lack of a wait_event. Found in: linux_kernel, Version: 4.14.59

CVE-2022-45885 [redacted] **MEDIUM (6.1)**
[https://reinhausen.atlassian.net/\[redacted\]](https://reinhausen.atlassian.net/[redacted])
An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_frontend.c has a race condition that can cause a use-after-free when a device is disconnected. Found in: linux_kernel, Version: 4.14.59

CVE-2022-45886 [redacted] **MEDIUM (6.1)**
[https://reinhausen.atlassian.net/\[redacted\]](https://reinhausen.atlassian.net/[redacted])
An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a disconnect versus dvb_device_open race condition that leads to a use-after-free. Found in: linux_kernel, Version: 4.14.59

CVE-2022-45888 [redacted] **MEDIUM (5.5)**
[https://reinhausen.atlassian.net/\[redacted\]](https://reinhausen.atlassian.net/[redacted])
An issue was discovered in the Linux kernel through 6.0.9. drivers/char/xillybus/xillyusb.c has a race condition and use-after-free during physical removal of a USB device. Found in: linux_kernel, Version: 4.14.59

CVE-2022-45887 [redacted] **LOW (2.9)**
[https://reinhausen.atlassian.net/\[redacted\]](https://reinhausen.atlassian.net/[redacted])
An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory leak because of the lack of a dvb_frontend_detach call. Found in: linux_kernel, Version: 4.14.59

IT-Sec CVE TODO-Review — Edited Save Details

MR-CERT Bug Analysis, Categorization, IN_PR... Assignee: All + More Contains text Search Switch to JQL

1-25 of 25

| Created | Components | SW-Component ↑ | Summary | CVSS Base Score | CVSS Environmental Score | Assignee | P | Status |
|-----------|------------|----------------|-------------------------------|-----------------|--------------------------|------------|---|-------------|
| 31/May/22 | CAP | core | CVE-2021-4231 | 5.4 | 5.5 | [redacted] | = | ANALYSIS |
| 31/May/22 | ISM | core | CVE-2021-4231 | 5.4 | 5.5 | [redacted] | = | ANALYSIS |
| 31/May/22 | ISM | ini | CVE-2020-7788 | 7.3 | | Unassigned | = | ANALYSIS |
| 31/May/22 | CAP | ini | CVE-2020-7788 | 7.3 | | Unassigned | = | IN_PROGRESS |
| 15/Aug/22 | ISM | libtar | CVE-2021-33643 | 9.1 | 5.6 | Unassigned | = | ANALYSIS |

Projects / MR-CERT / [redacted]

CVE-2022-45884

Attach Create subtask Link issue Katalon Manual Tests (BETA)

Description
An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c has a use-after-free, related to dvb_register_device dynamically allocating fops.
Found in: linux_kernel, Version: 4.14.59

Web links
lore.kernel.org
lore.kernel.org

Activity
Show: All Comments History Work log Newest first

Add a comment...
Pro tip: press **M** to comment

Details

Components [redacted]

Affects versions 1.01

Assignee Unassigned
[Assign to me](#)

Reporter [redacted]

CVSS Base Score 7

CVSS Environmental Score 6.1

Vector String <https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AVL/ACH/PR/L/UI/N/S:U/CH/IR/A/H/CR/M/IR/L/AR/L>

SW-Component linux_kernel

SW-Component-Version 4.14.59

Tools: <https://github.com/cve-search/cve-search>

Schwachstellenmanagement – ein kurzer Überblick

Beispiel Security Advisory



Product CERT

MR-CERT

A dedicated cybersecurity emergency response team (CERT) at MR is the central point of contact for all questions relating to IT security. The MR specialists advise customers and are involved in the development of new products from the outset. Among other things, they determine which standards and guidelines have to be observed for a specific project.

Security Advisories

Here you can find important security advisories for our automation products:

Security Advisory MRSA-2021-1201:

→ [Software vulnerability log4j](#) (Version 5.0 - Jan 28th, 2022)

Security Advisory MRSA-2022-0801:

→ [Software vulnerability in ETOS/ISM SW 3-3](#)
(Version 1.3 - Sep 22, 2022)

MR Product CERT: ProductCERT@reinhausen.com



Security Advisory MRSA-2022-0801: Software vulnerability in ETOS/ISM SW 3-3 Version 1.3 - 22.09.2022

Summary

A vulnerability has been identified in the SW 3-3 assembly of ETOS® and further ISM® based products. An attacker could exploit this vulnerability by crafting a special HTTP request message to fully compromise the target device.

The vulnerability documented in CVE-2020-6994 is classified with a CVSS score of 9.8 [1].

Maschinenfabrik Reinhausen GmbH provides its customers with products of high quality and therefore this Security Advisory shall inform you about status and possible remediation.

Products

| | |
|-------------------|---|
| Products: | ETOS/ISM – all versions |
| Product assembly: | SW 3-3 |
| Vulnerable: | SW 3-3-Hirschmann PRP and HSR (HiOS) Software 07.0.02 and lower |
| Recommended: | HiOS Software 07.0.03 and higher, latest version: 07.1.05 |

Description

Maschinenfabrik Reinhausen was informed of a vulnerability report that affects the SW 3-3 assembly of the ETOS® and ISM® series. The SW 3-3 assembly is included if the Parallel Redundancy Protocol (PRP) or High-availability Seamless Redundancy (HSR) is ordered. The SW 3-3 assembly is based on the Belden/Hirschmann EES-25 ethernet switch.

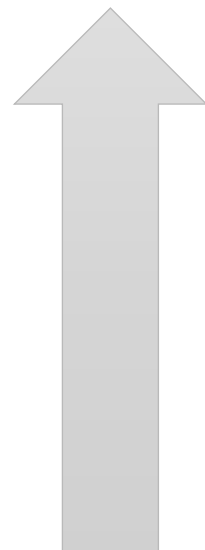
Schwachstellenmanagement

Beispiel MR ETOS - Prozess



Prüfung Software: täglich
Review: wöchentlich
Kennzahlen: pro Quartal
(ISMS Management Report)

- | Inventar und
- | Informationen über Schwachstellen
- | einholen & bewerten



- | Schwachstellen kommunizieren (Security Advisories)
- | Produkt (Software) Updates

Advisories: Bei Bedarf
SW-Updates: 3x im Jahr

Schwachstellenmanagement Kennzahlen



+ Im Rahmen des MR Vulnerability Management Prozesses (VMP) wurden im Berichtszeitraum **57 neue** Software-Schwachstellen (CVEs) identifiziert und bewertet (Zuletzt: 32).

| Anzahl von Summary | 1 | 2 | 3 | 4 | Gesamtergebnis |
|-----------------------|----------|------------|------------|-----------|----------------|
| ⊕ 2020 | 3 | 19 | 89 | 7 | 118 |
| ⊕ 2021 | | 40 | 100 | 5 | 145 |
| ⊖ 2022 | 2 | 62 | 308 | 14 | 386 |
| ⊕ Qrtl1 | | 13 | 114 | 6 | 133 |
| ⊕ Qrtl2 | 2 | 30 | 85 | 7 | 124 |
| ⊕ Qrtl3 | | 14 | 82 | 1 | 97 |
| ⊕ Qrtl4 | | 5 | 27 | | 32 |
| ⊖ 2023 | | 7 | 39 | 11 | 57 |
| ⊕ Qrtl1 | | 7 | 39 | 11 | 57 |
| Gesamtergebnis | 5 | 128 | 536 | 37 | 706 |

| Priorität: |
|------------|
| 1 highest |
| 2 high |
| 3 medium |
| 4 low |
| 5 lowest |





Schwachstellenmanagement

Ausblick: Web-Umfeld und eigene Produkte

Ausblick, hier nicht abgedeckt:

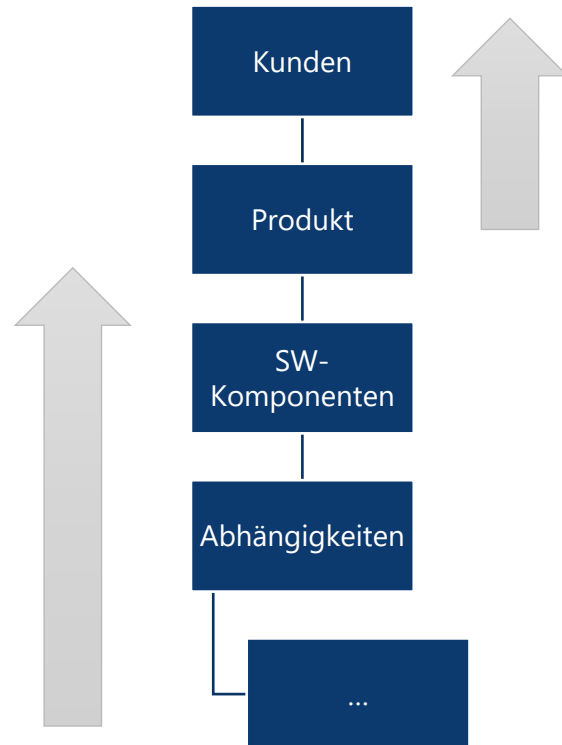
- + Schwachstellen im Web-Umfeld (Node.js, NPM etc.) bzw. mit Paketmanager (pip etc.):
 - Hohe Komplexität und Dynamik
 - Braucht geeignete Schwachstellenscanner, oft keine CVEs vorhanden -> z.B. Snyk, Mend, BlackDuck etc.
 - Einbinden in bestehende Prozesse mit Analyse und Meldung ist nötig, nicht nur Pull-Requests stellen

- + Schwachstellen in eigenen Produkten:
 - Statische Code-Analysen
 - Dynamische Code-Analysen
 - Code-Reviews
 - Security-Protokollierung – Integration in SIEM Systeme

Schwachstellenmanagement

Ausblick: Prozess-Automatisierung mit CSAF

+ Common Security Advisory Framework (CSAF)



CSAF-Standard für maschinenverarbeitbare Security Advisories

- Erfolgreiche Zusammenarbeit zwischen deutschem BSI und schweizerischem Cyber-Defense Campus (CYD)
- Zwei Proof-of-Concepts (PoCs) zur Erstellung und Verwaltung von CSAF-Dokumenten werden sukzessive zu vollständigen Open-Source-Tools weiterentwickelt
- So können in Zukunft Betreiber, Hersteller und Behörden aller Länder effizienter Schwachstellen-Informationen austauschen und ihre Cyber-Sicherheit verbessern

Schwachstellenmanagement

Ausblick: Software Bill of Materials (SBOM)

+ Diverse gesetzliche Anforderungen, u.a.
 EU Cyber Resilience Act, US CISA / White House Executive Order

+ Formate:

- Cyclone DX
- SPDX
- Weitere -> MR

+ Tools:

- Viele!
- TODO: Überblick, Forschung
- KISS!

+ Mehr Informationen:

- [BSI - Presse - SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette](#)
- [Executive Order on Improving the Nation's Cybersecurity | The White House](#)
- [Software supply chain - Wikipedia](#)



Quelle: <https://scribesecurity.com/sbom/#definition-of-software-bill-of-materials>

Schwachstellenmanagement

Zusammenfassung

- + Über die Maschinenfabrik Reinhausen GmbH
- + Anforderungen im KRITIS-Umfeld
- + Übersicht, Hintergrund / Auslöser: log4j
- + Architektur
 - Software Component Analysis
 - SBOM – Software Bill of Materials
 - Beispiel: MR-SBOM
- + Identifizierung und Bewertung von Schwachstellen
 - Von der Komponente zur Schwachstelle
 - Automatisierung im MR-CERT
 - Security Advisories
 - Prozess & Kennzahlen
- + Ausblick: Automatisierung CSAF, SBOM
- + Praktische Übungen



Werkstudenten gesucht!

Bereich Informatik, Wirtschaftsinformatik, Elektro- und Informationstechnik

- + SBOM – Software Bill of Materials:
 - Tools
 - Formatkonvertierungen
 - Automatisierung

- + ISMS auf Basis ISO 27001:
 - Abdeckung der Norm-Dokumente
 - Vollständigkeit der Dokumentation zur Umsetzung
 - Abgleich zwischen Dokumentation und Risikomanagement
 - Detail-Ausarbeitung einzelner Themen aus den Bereichen Technik, Organisation, Sensibilisierung

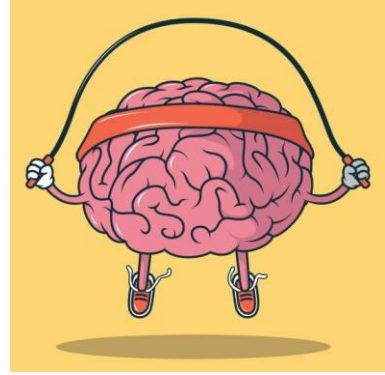
Kontakt:

Dr. Hubert Feyrer

E-Mail: h.feyrer@reinhausen.com



Praktische Übungen - Einzelaufgaben

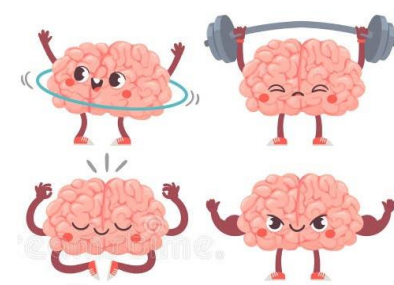


1. Quellenrecherche zu Schwachstellen:
 - a) <https://nvd.nist.gov>, BSI, CISA – Was macht die ENISA?
 - b) Welche Beschreibungen existieren jeweils für log4j?
 - c) Welche Schwachstelle beschreibt CVE-2019-14287? Welche Systeme sind betroffen? Wie zu reparieren?
 - d) Sie haben eine Schwachstelle gefunden. Wie erhalten Sie eine CVE-Nummer dafür? Wovon hängt das Vorgehen ab? ([Video](#))

2. CPEs: Gegeben CPE – CVEs suchen
 - a) Welche Informationen finden Sie zu `cpe:2.3:a:sudo_project:sudo:1.8.7`?
 - b) Wie kann die Schwachstelle in CVE-2019-14287 ausgenutzt werden? Tip: www.exploit-db.com
 - c) Wie ist der CPE zu Microsoft's Azure-CLI Tools? Welche Schwachstellen existieren? Welche Abhilfen?

3. CVSS: Bewertung von Schwachstellen
 - a) wie ist der Schweregrad beiden oben genannten Schwachstellen Azure CLI Tools, CVE-2019-14287?
 - b) Nach welchen Kriterien wird dabei unterschieden?

Praktische Übungen - Gruppenaufgaben (max. 4)



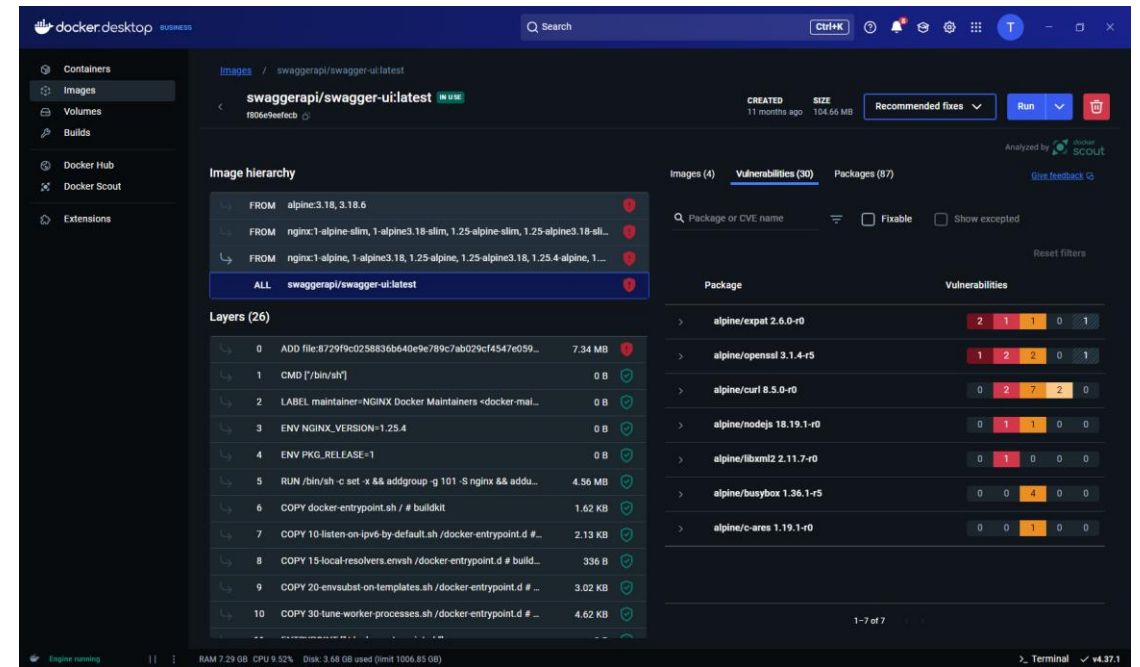
1. SBOM Tools: Welche Werkzeuge existieren zur Analyse und Erstellung von SBOMs?
 - a) ... für ein fertiges Binary wie z.B. <https://download.gimp.org/gimp/v2.10/windows/gimp-2.10.38-setup-1.exe>
 - b) ... für einen Docker-Container Ihrer Wahl?
 - c) ... für ein per buildroot selbst gebautes Linux? Was bietet yocto Linux?

2. SBOM Formate:
 - a) Mit welchen Werkzeugen kann von SPDX nach Cyclone DX konvertiert werden?
 - b) Bieten beide Formate die gleichen Möglichkeiten? Wo sind Grenzen? Welche weiteren / eigenen Formate existieren?

3. CSAF:
 - a) Welche Möglichkeiten bietet CSAF zur Erkennung und Bewertung von Schwachstellen?
 - b) Welche Werkzeuge existieren? Wie werden (teil-)automatisiert Security-Advisories erstellt / vorbereitet?

Praktische Übungen - Eigenrecherche & Denkanstöße

- + Welche Möglichkeiten für Schwachstelleninformationen und Updates bietet welches Framework / Tool etc.
 - [Configuring Dependabot security updates - GitHub Docs](#)
 - [UnattendedUpgrades - Debian Wiki](#)
 - [pip-audit · PyPI](#)
 - [npm-audit | npm Docs](#)
 - [About RustSec › RustSec Advisory Database](#)
 - Docker Desktop (siehe Bild rechts)
 - Für C++? E.g. boost oder std?
 - Für Java? Go? ...
- + Wie kann man das tägliche Scannen / Prüfen automatisieren?
- + Wie kommen Informationen (Advisories, Updates) gezielt an den Kunden?



**THE POWER
BEHIND POWER.**
reinhausen.com

