Schwachstellenmanagement für IoT-Produkte im Energiesektor

12.09.2023 Dr. Hubert Feyrer, Thilo Böhm

Schwachstellenmanagement
Sprecher

Dr. Hubert Feyrer ist Cyber Security-Experte bei der Maschinenfabrik Reinhausen. Nach einem Studium in technischer Informatik und Promotion in Informationswissenschaften war er u.a. tätig als Systembetreuer, Hard- und Softwareentwickler, IT-Leiter sowie als Chief Information Security Officer (CISO).

Thilo Böhm ist Security-Architekt im Bereich der IoT-Entwicklung. Bereits während seines Masterstudiums war er für die Sicherheit von Energienetzen bei MR tätig und initiierte 2018 das MR-CERT.

Schwachstellenmanagement Agenda

- Über die Maschinenfabrik Reinhausen GmbH
- 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

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%

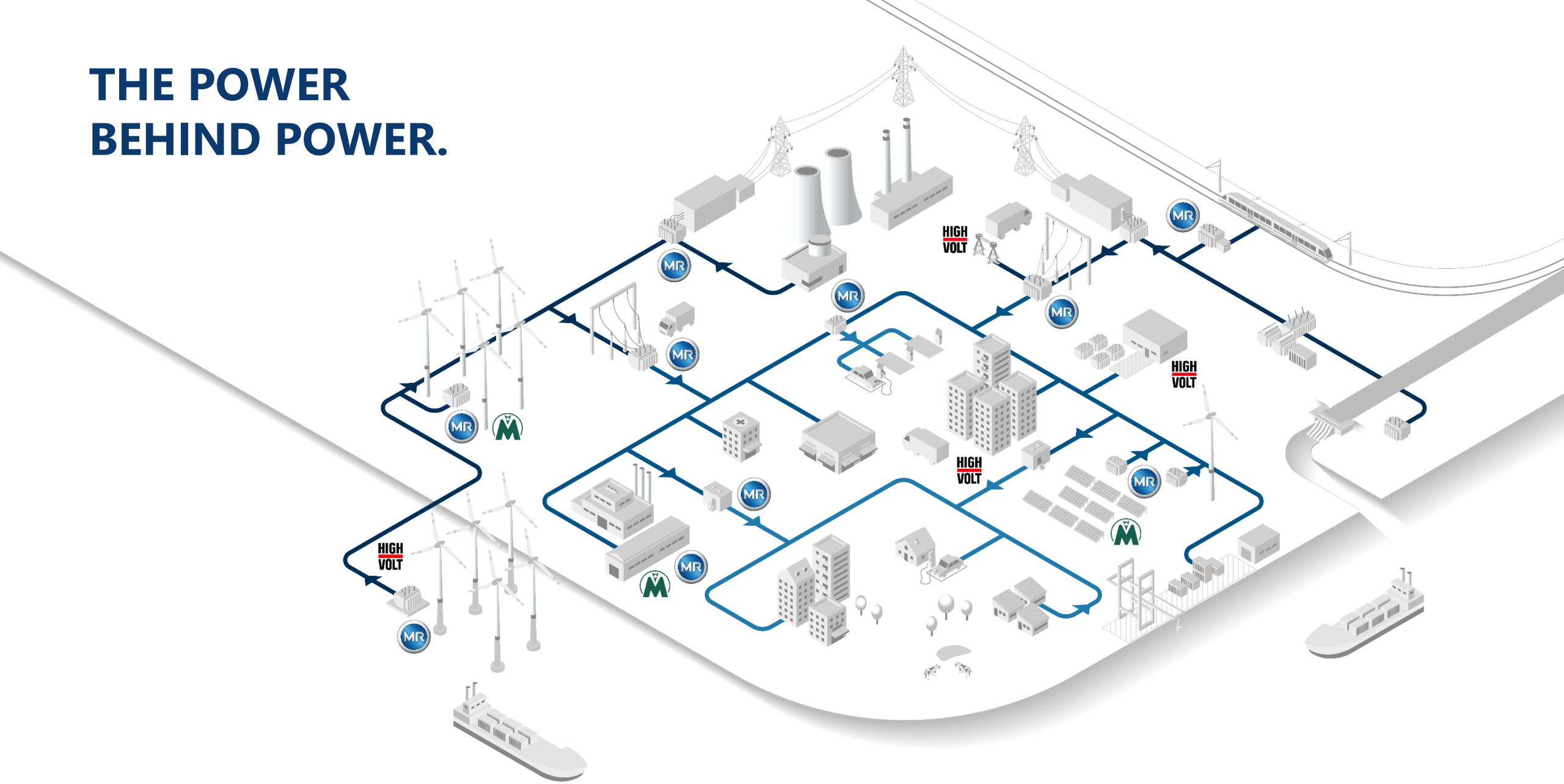
aller Produkte noch in Betrieb,
der älteste OILTAP seit 1950

Präsent in aller Welt

8.000

Kunden
in 185 Ländern

THE POWER BEHIND POWER.



Anerkannt und ausgezeichnet

top EMPLOYER DEUTSCHLAND GERMANY 2022

Top 2022 Company kununu

GREAT PLACE TO WORK. 2017 Beste Arbeitgeber Deutschland

Der Deutsche Innovationspreis

ees AWARD 2019 WINNER

GERMAN DESIGN AWARD WINNER 2017

INNOVATIONSPREIS DER DEUTSCHEN WIRTSCHAFT

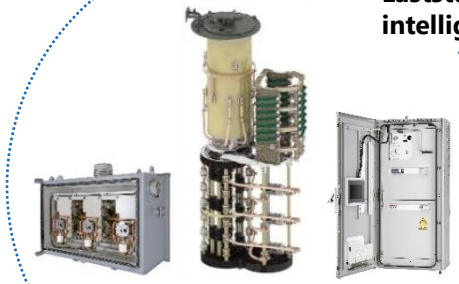
reddot award 2015 winner

innovationspreis Bayern 2014

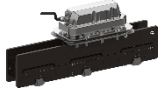
BEST INNOVATOR 2012/2013

Lösungen für Lastfluss und Spannungsqualität

Transformatoren-Zubehör



Laststufenschalter & intelligente Antriebe

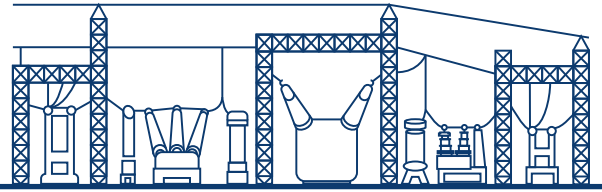


Regeltechnik für Verteiltransformatoren

Dienstleistungen im Umspannwerk

Sensorik, Automatisierung, Digitalisierung

OEM & Systemintegratoren



Netzbetreiber

Lasten & Einspeiser

Hochspannungs-Isolatoren

Hochspannungs-prüftechnik

Power Quality Lösungen

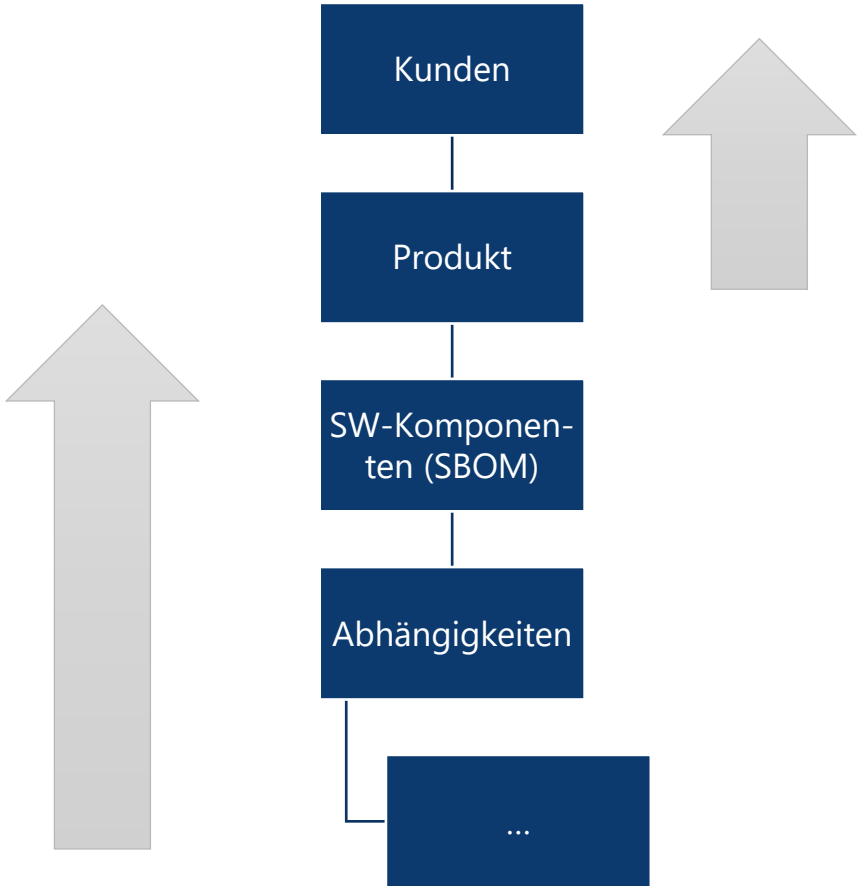
Leistungselektronische Systeme & Komponenten

Drosseln Mittel- & Niederspannung

Schwachstellenmanagement

Schwachstellenmanagement
Übersicht

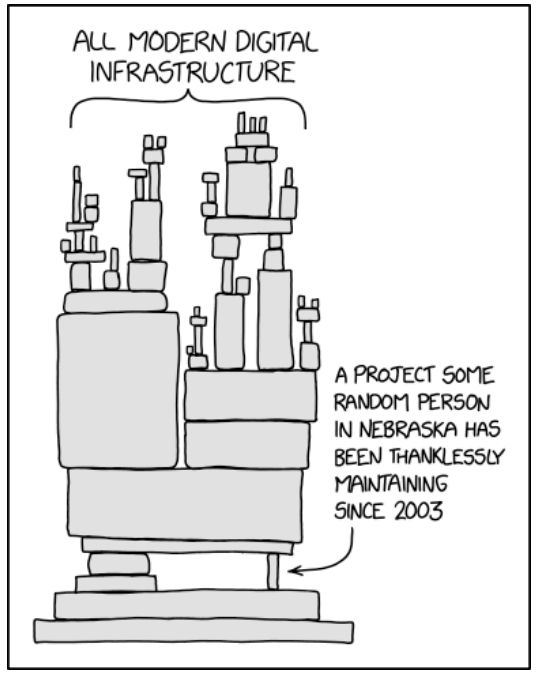
- Inventar und
- Informationen über Schwachstellen
- einholen & bewerten

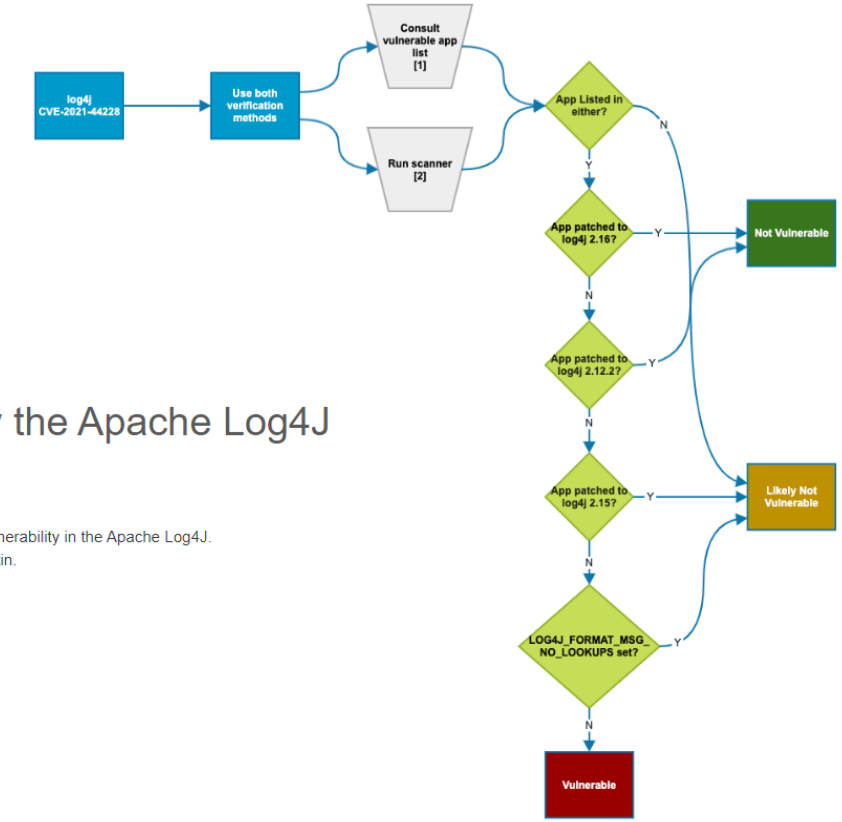


- Schwachstellen kommunizieren (Security Advisories)
- Produkt (Software) Updates

Schwachstellenmanagement log4j

+ Hintergrund / Auslöser: log4j

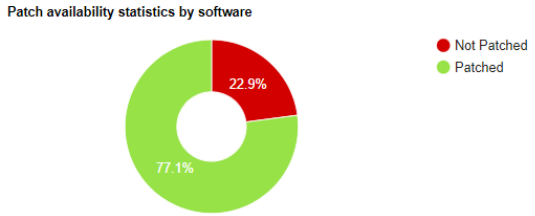




List of vendors and software affected by the Apache Log4J vulnerability (CVE-2021-44228)

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



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**		


THE WHITE HOUSE

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

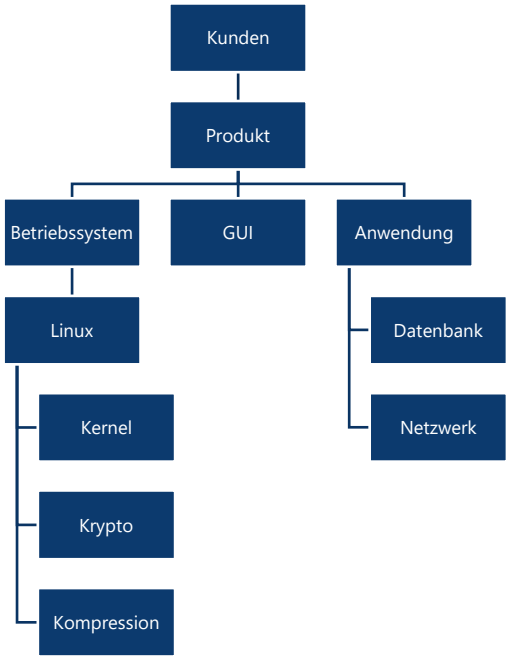
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

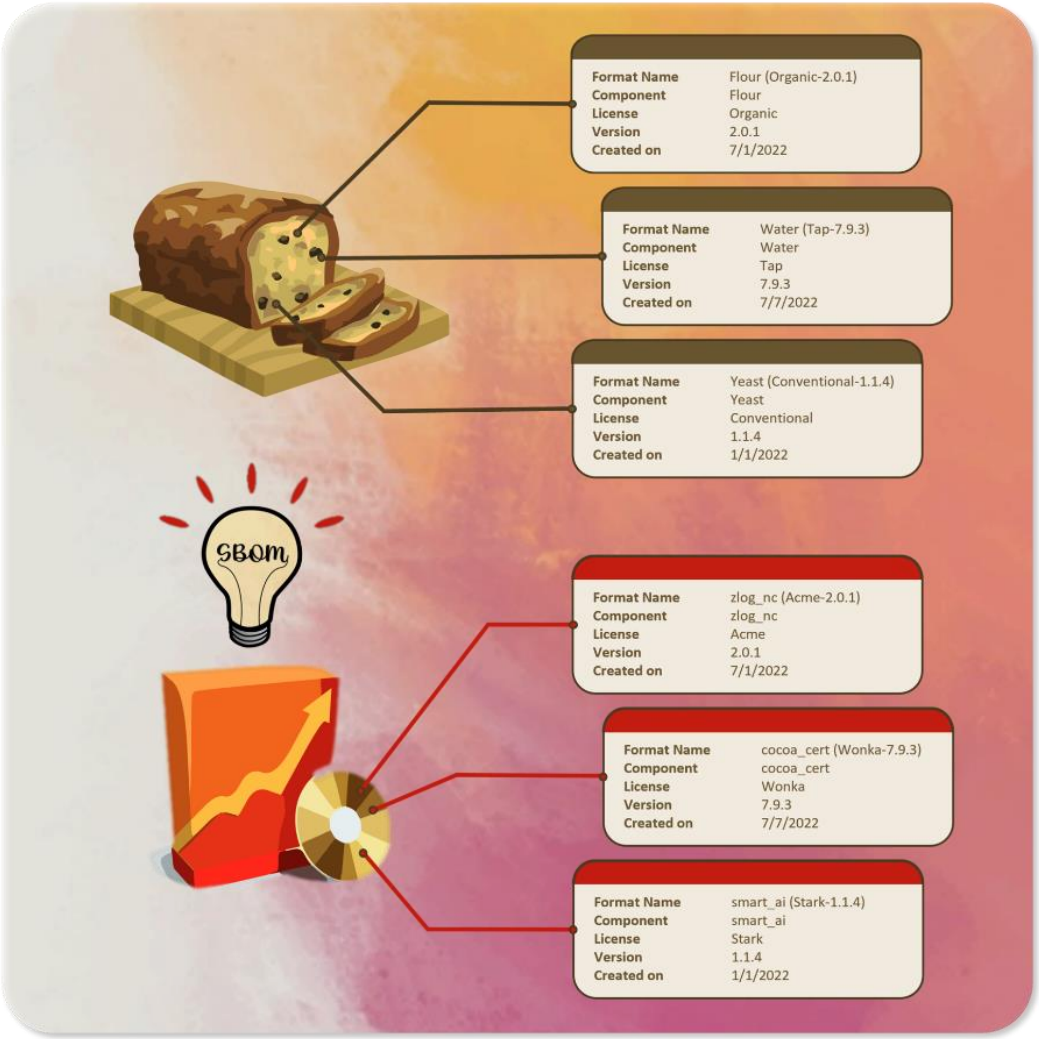
Quellen: https://xkcd.com/2347/
https://www.cybersecurity-help.cz/reports/ApacheLog4J.php
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Schwachstellenmanagement Architektur

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

+ Beispiel:

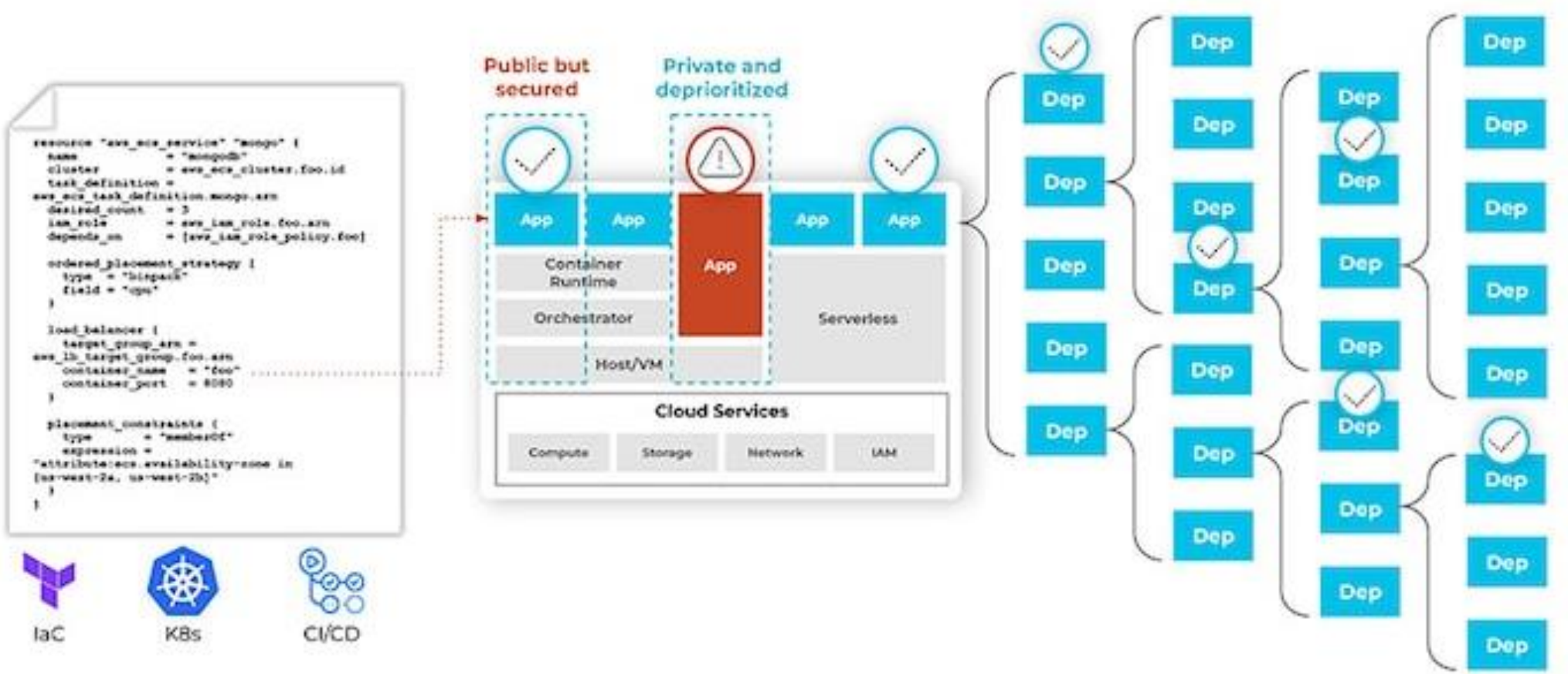




Quellen:
https://www.splunk.com/en_us/blog/industries/harmonizing-the-federal-effort-on-automating-software-bill-of-materials.html

Schwachstellenmanagement
Identifizierung von Schwachstellen

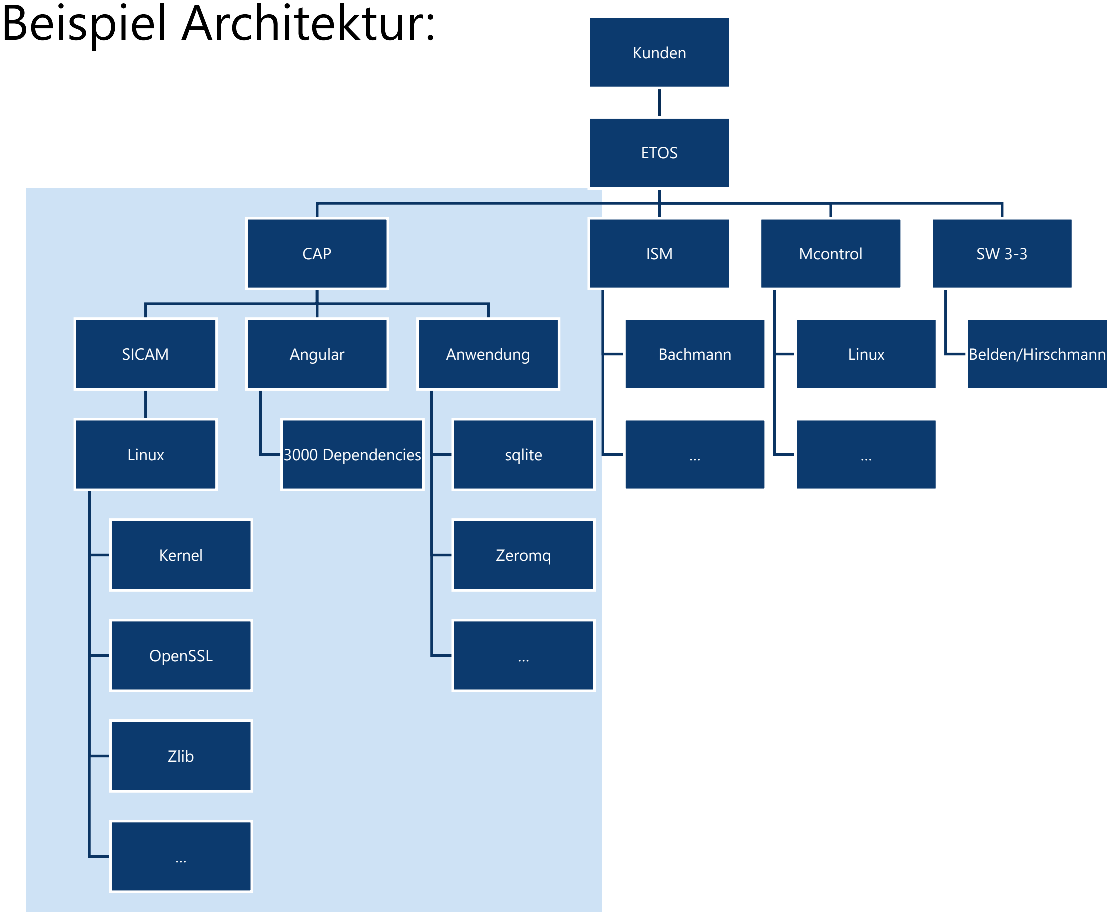
+SCA – Software Component Analysis – Software: z.B. Black Duck, snyk, mend

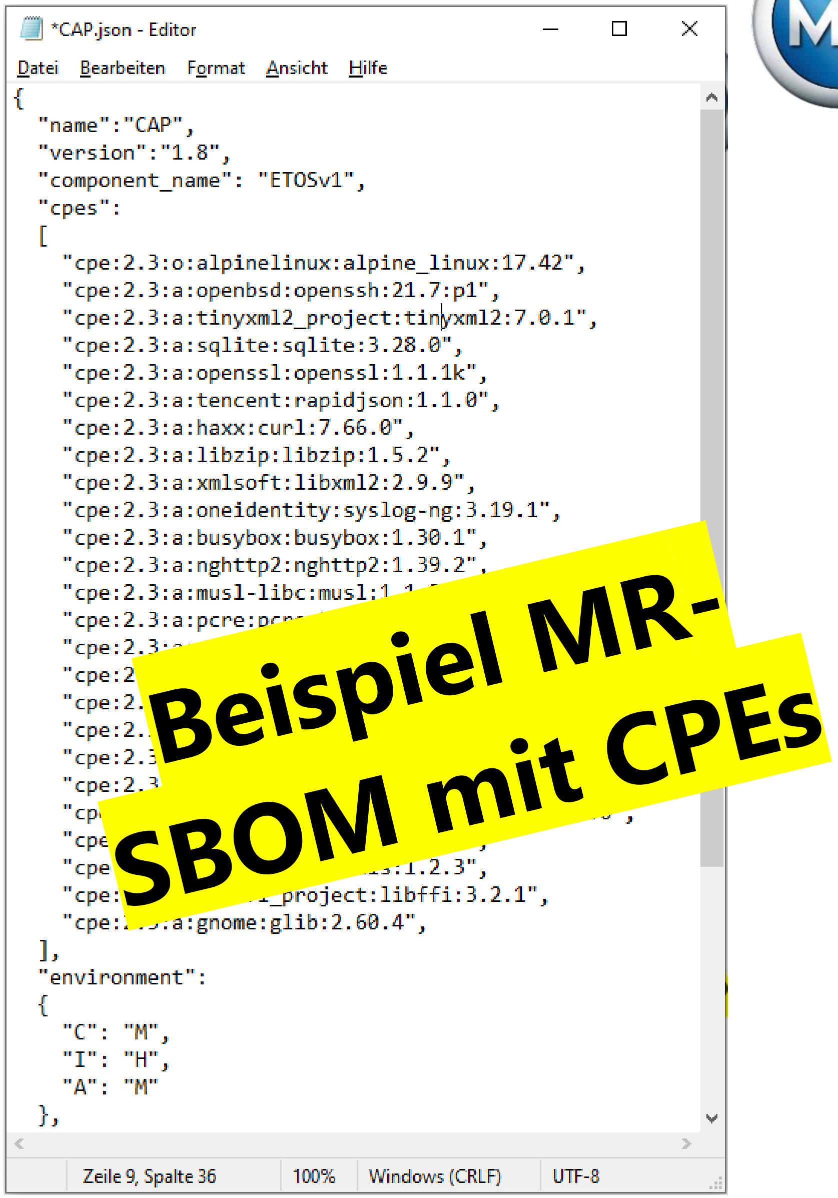


Quellen: https://www.paloaltonetworks.com/cyberpedia/what-is-sca

Schwachstellenmanagement
Beispiel - Architektur & SBOM

+ Beispiel Architektur:





Quellen:

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

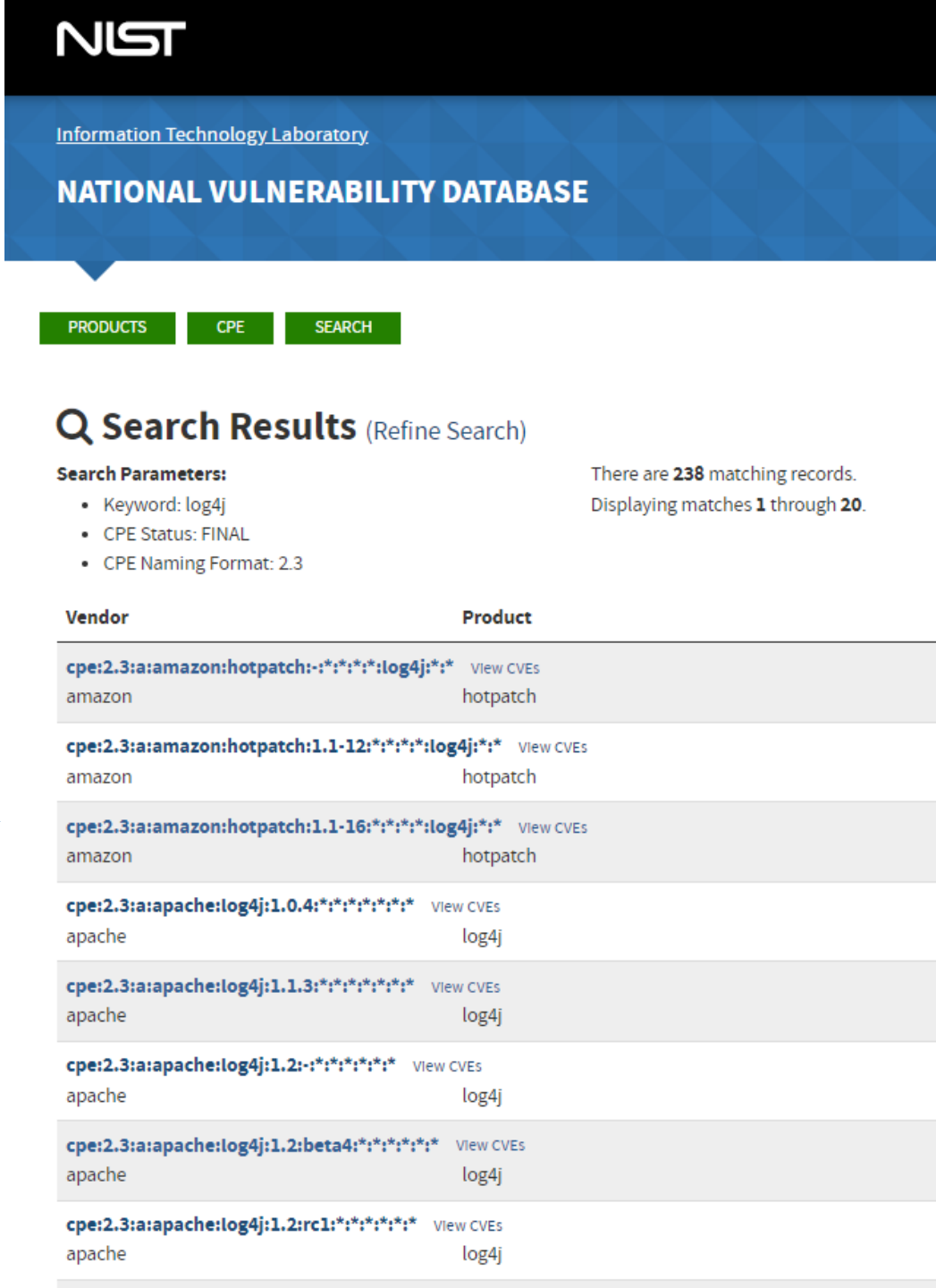
Schwachstellenmanagement
Identifizierung von Komponenten

+ 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:

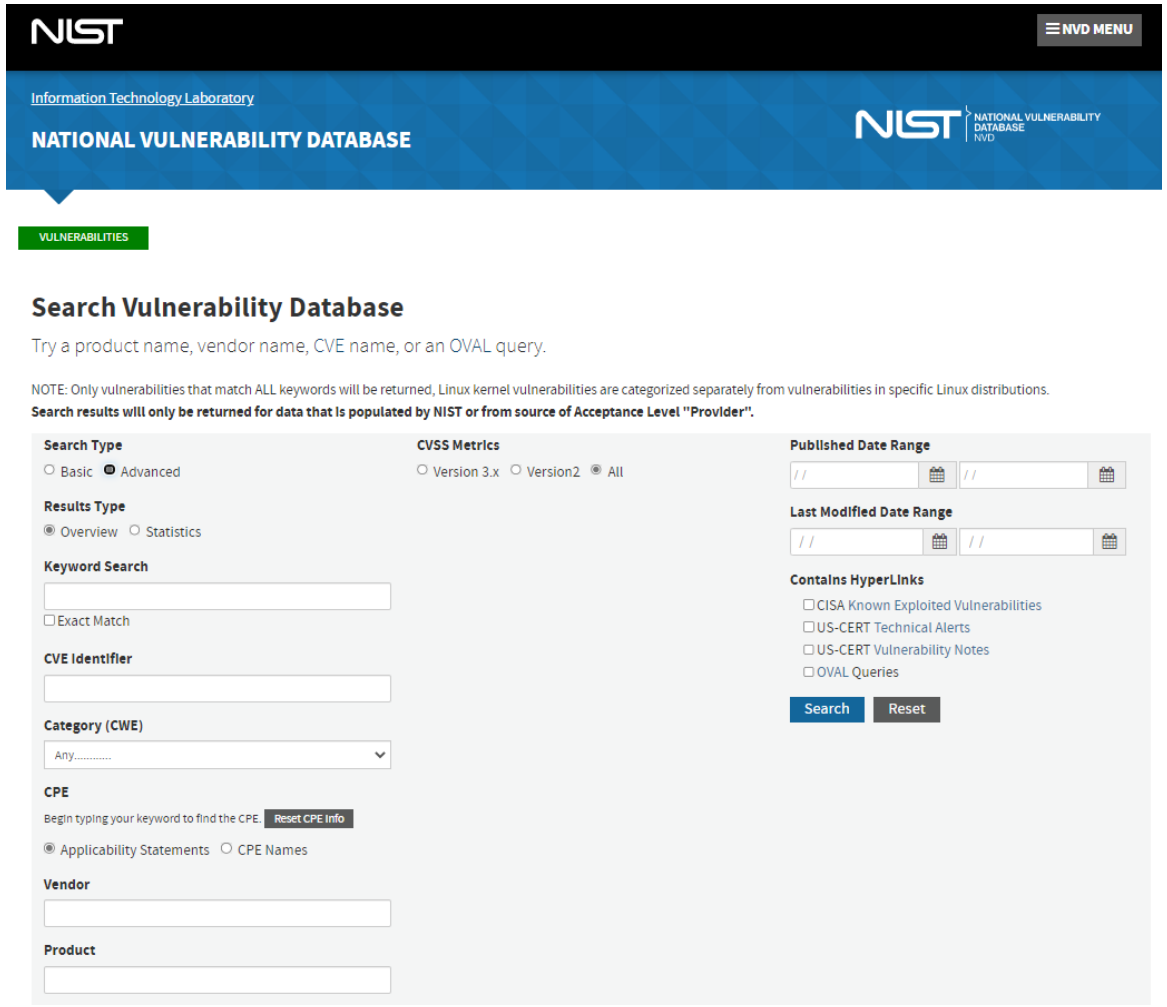
Alternativen:

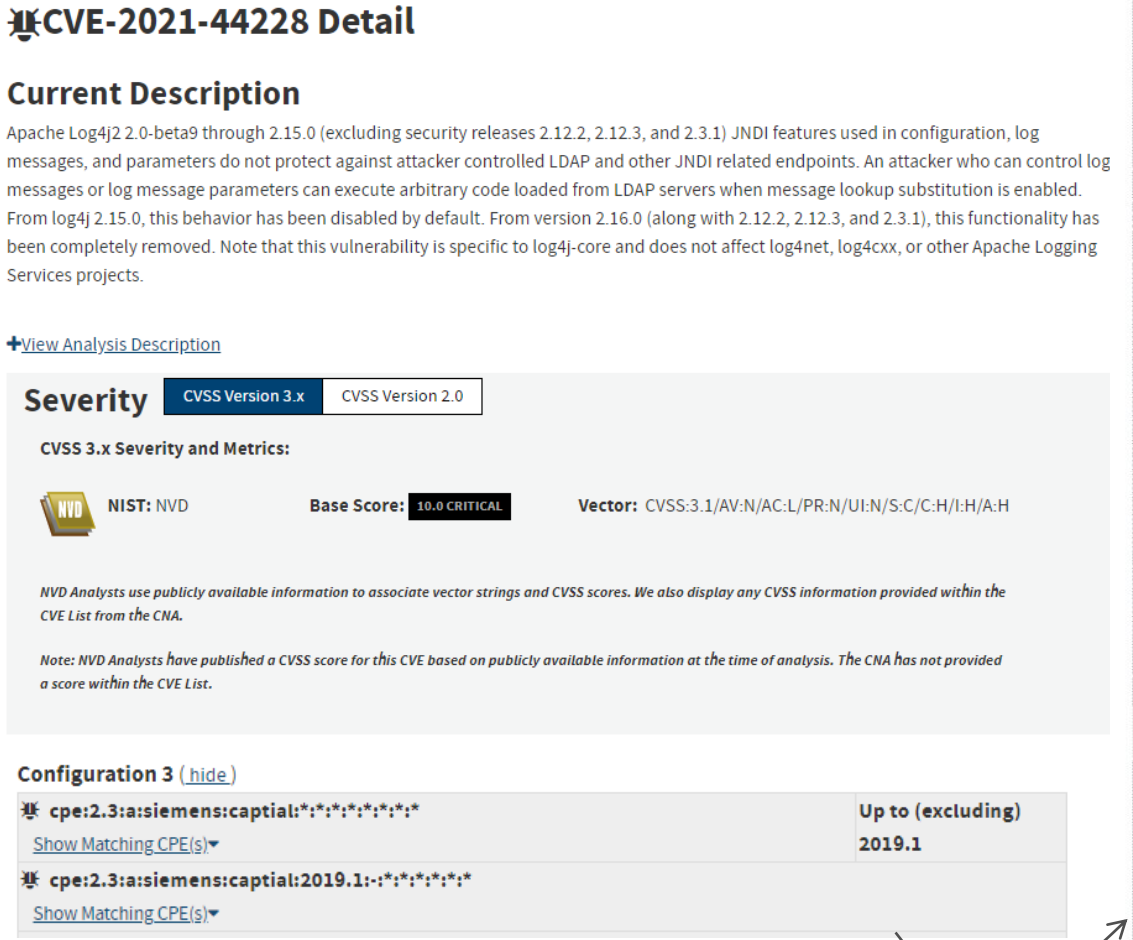
- PURL: Package URLs, primär node.js Umfeld, kein Mapping zu CPEs, CVEs
- SWID: ISO/IEC 19770-2:2015, nur Theorie



Schwachstellenmanagement
Identifizierung von Schwachstellen

+CVE - Common Vulnerability Enumeration:

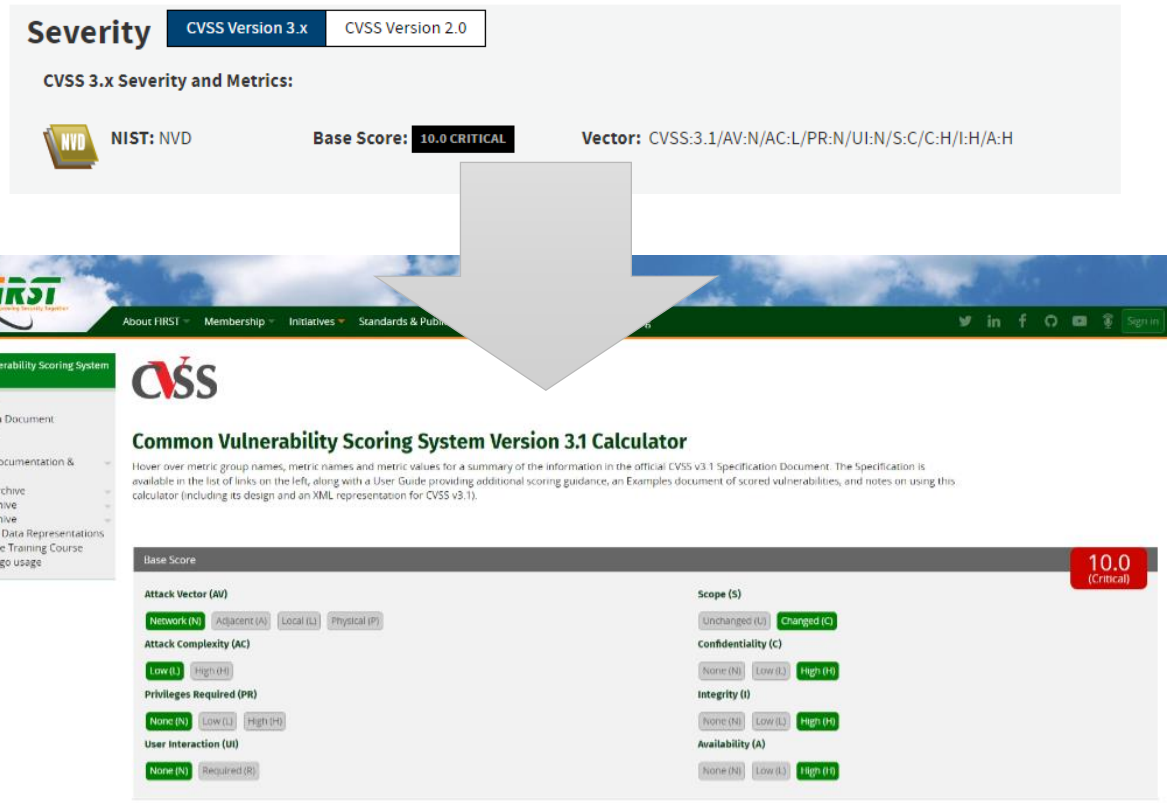


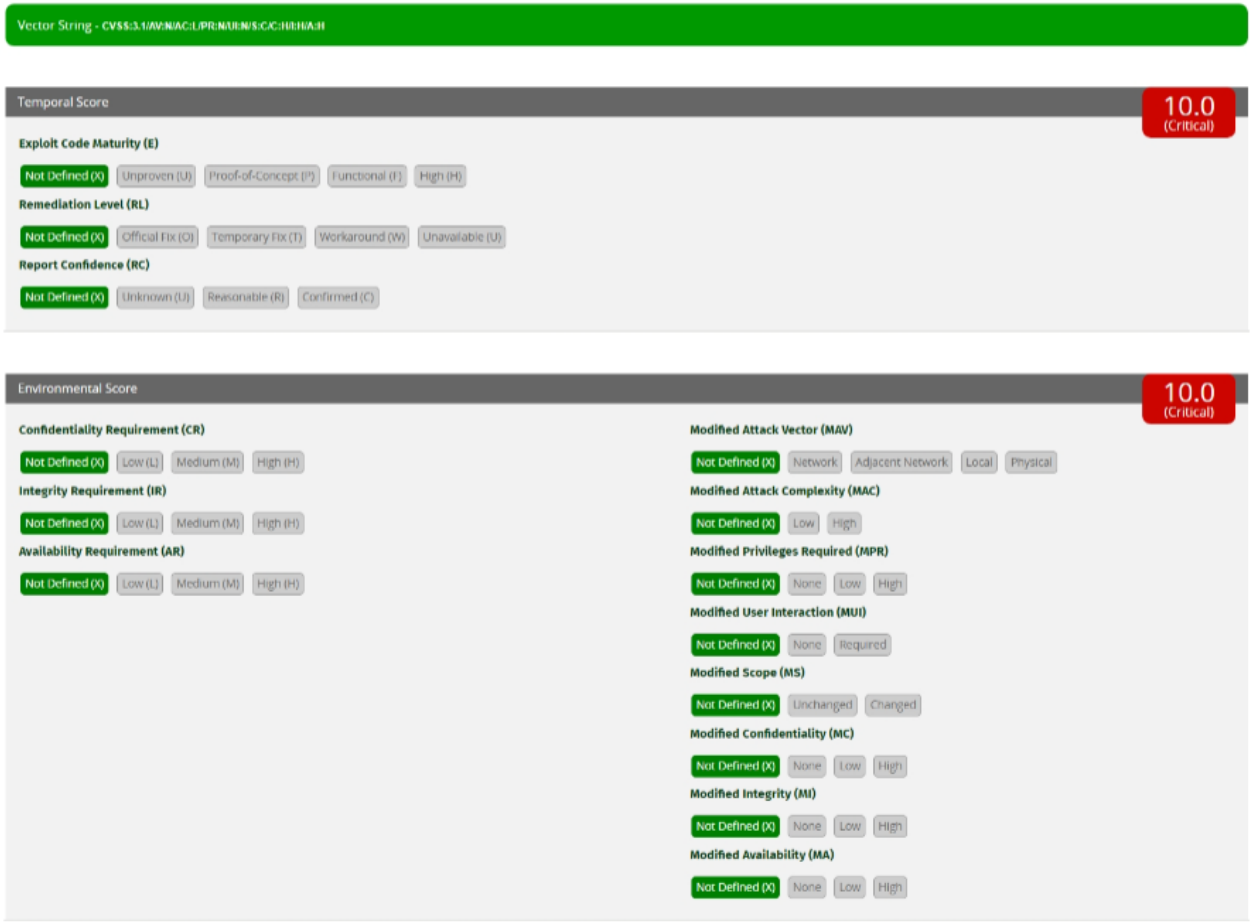


- Quellen: https://nvd.nist.gov/vuln/search
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Schwachstellenmanagement
Bewertung von Schwachstellen

+CVSS – Common Vulnerability Scoring System:

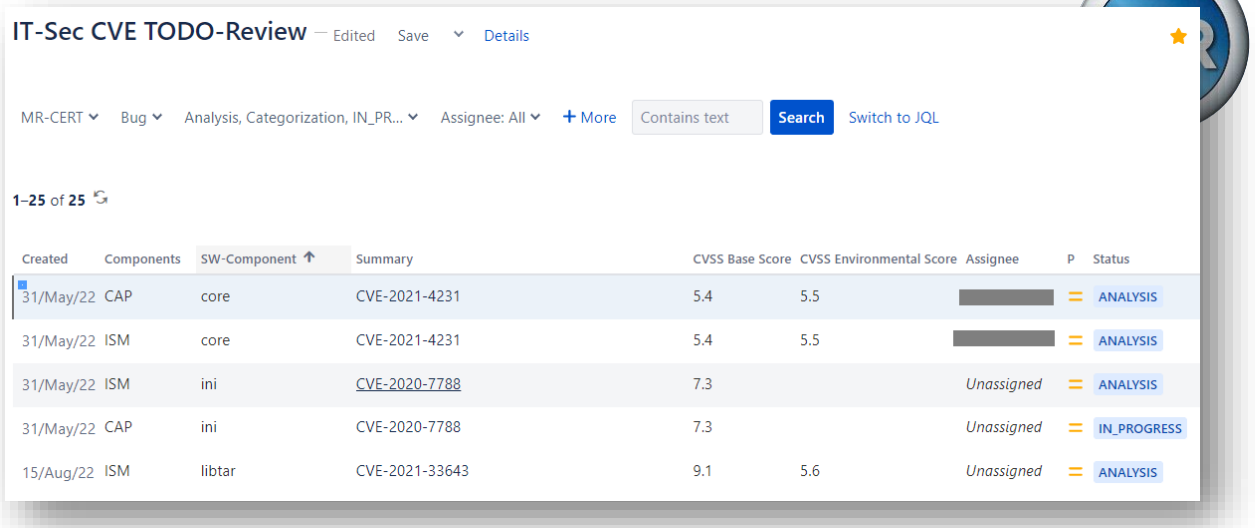


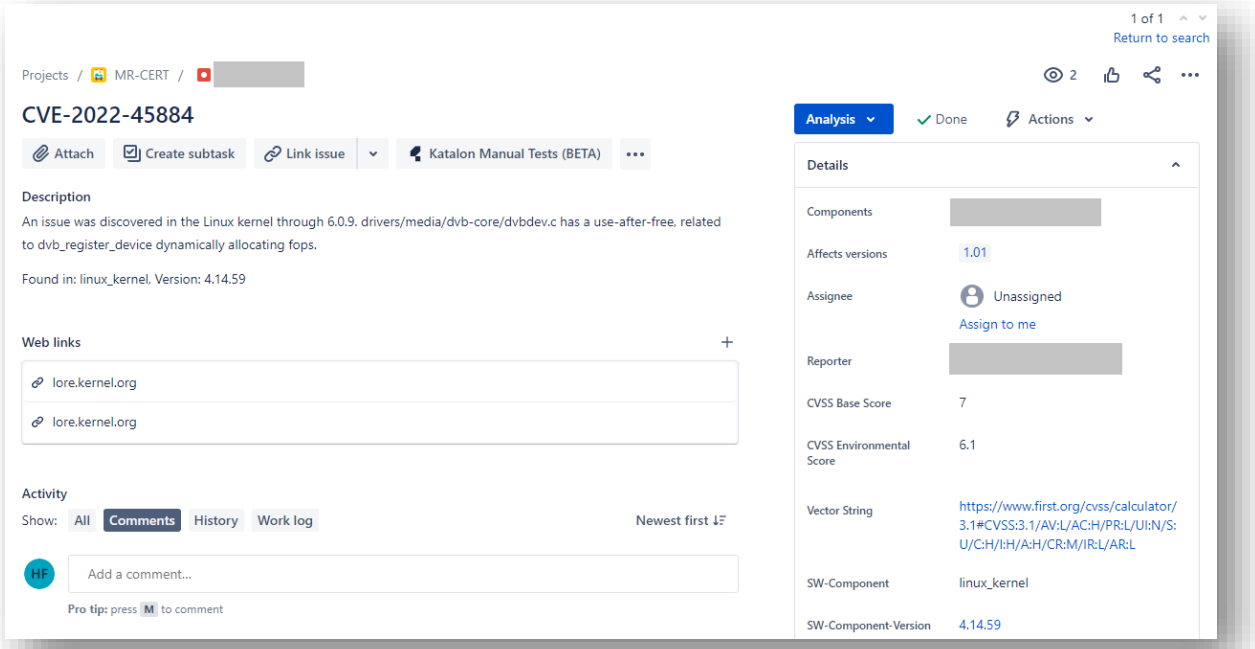


Quellen: https://nvd.nist.gov/vuln/search
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Schwachstellenmanagement Automatisierung MR-CERT

+ MR-CERT CVE Server, Email & Jira:





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

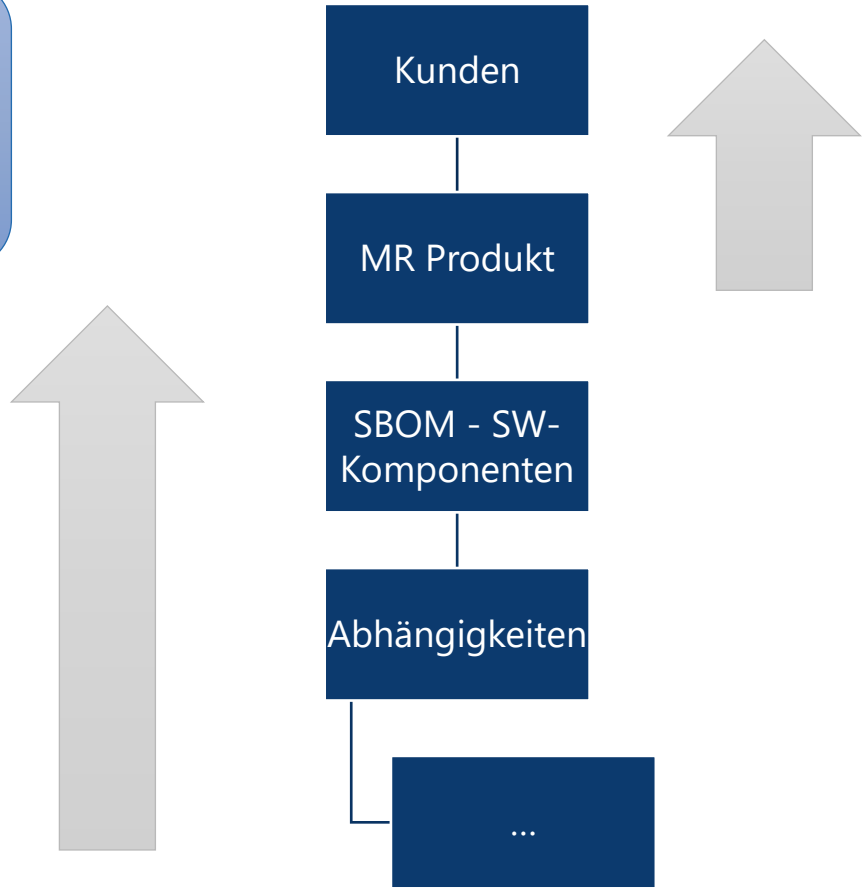
Maschinenfabrik Reinhausen was informed of a vulnerability report that affects the SW 3-3 assembly of the ETOS® and ISM® series. The SW 3-3 assembly is included if the Parallel Redundancy Protocol (PRP) or High-availability Seamless Redundancy (HSR) is ordered. The SW 3-3 assembly is based on the Belden/Hirschmann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

Quellen: https://www.reinhausen.com/servicedetail/transformer-digitalization/product-cert

Schwachstellenmanagement
Beispiel ETOS - Prozess

Prüfung Software: täglich
Review: wöchentlich
Kennzahlen: pro Quartal

- Inventar und
- Informationen über Schwachstellen
- einholen & bewerten



- Schwachstellen kommunizieren (Security Advisorys)
- Produkt (Software) Updates

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

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

Schwachstellenmanagement
Kennzahlen

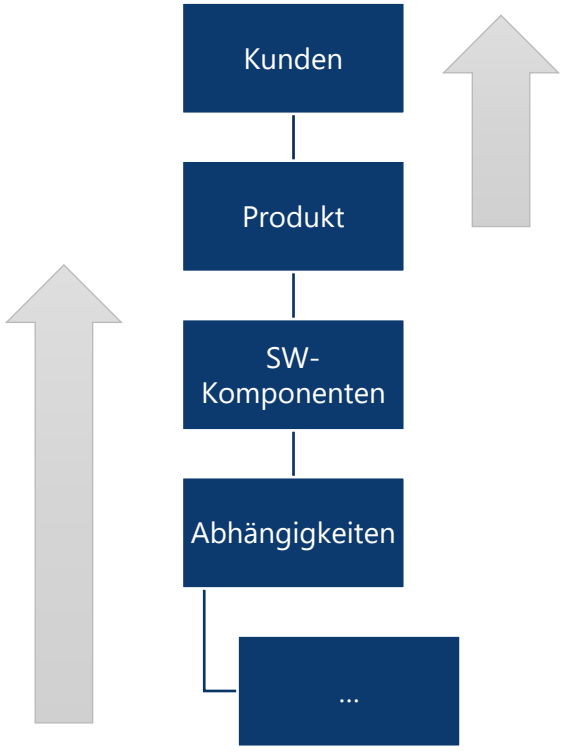
+Im Rahmen des MR Vulnerability Management Prozesses (VMP) wurden im Berichtszeitraum **57** neue Software-Schwachstellen (CVEs) identifiziert und bewertet (Zuletzt: 32).

Anzahl von Summary					
Zeilenbeschriftungen	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: 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

Bundesamt
für Sicherheit in der
Informationstechnik

Quellen: https://social.bund.de/@bsi/107564144878688776
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html

Schwachstellenmanagement Zusammenfassung

- Über die Maschinenfabrik Reinhausen GmbH
- 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

THE POWER BEHIND POWER.

reinhausen.com

Schwachstellenmanagement
Schematische Darstellung

Manuelle Schwachstellenüberwachung für nicht standardisierte Veröffentlichungen

+ Andere CERTs + Lieferanten

Automatisierte Schwachstellensuche mit MR-CVE-Search-Server für standardisiert veröffentlichte Lücken

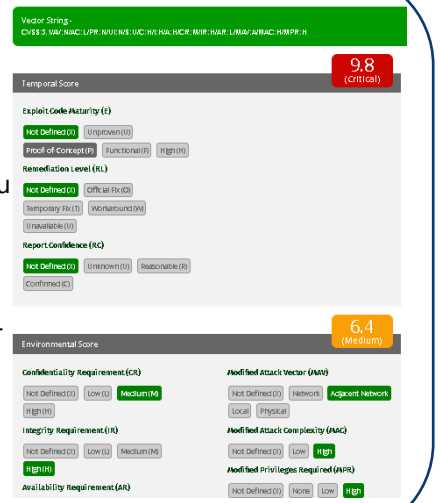
+ Produktname, Version,
+ [Liste an Software-Komponenten]

Sicherheitslücke in einem von MR verwendeten Produkt?

+ Quellcode,
+ Lieferantenauskunft
+ ...

Analyse

+ Klassifizierung der Sicherheitslücke unter Berücksichtigung der Umgebungsbedingungen durch standardisiertes Scoring (CVSS)
- ≥ 7 → High → SOFORT
- ≥ 4 → Medium → reg. Fix
- Sonst → Low



Kategorisierung

Behebung @ Fachabteilung

Ende

Jira Ticket States