TLP:CLEAR

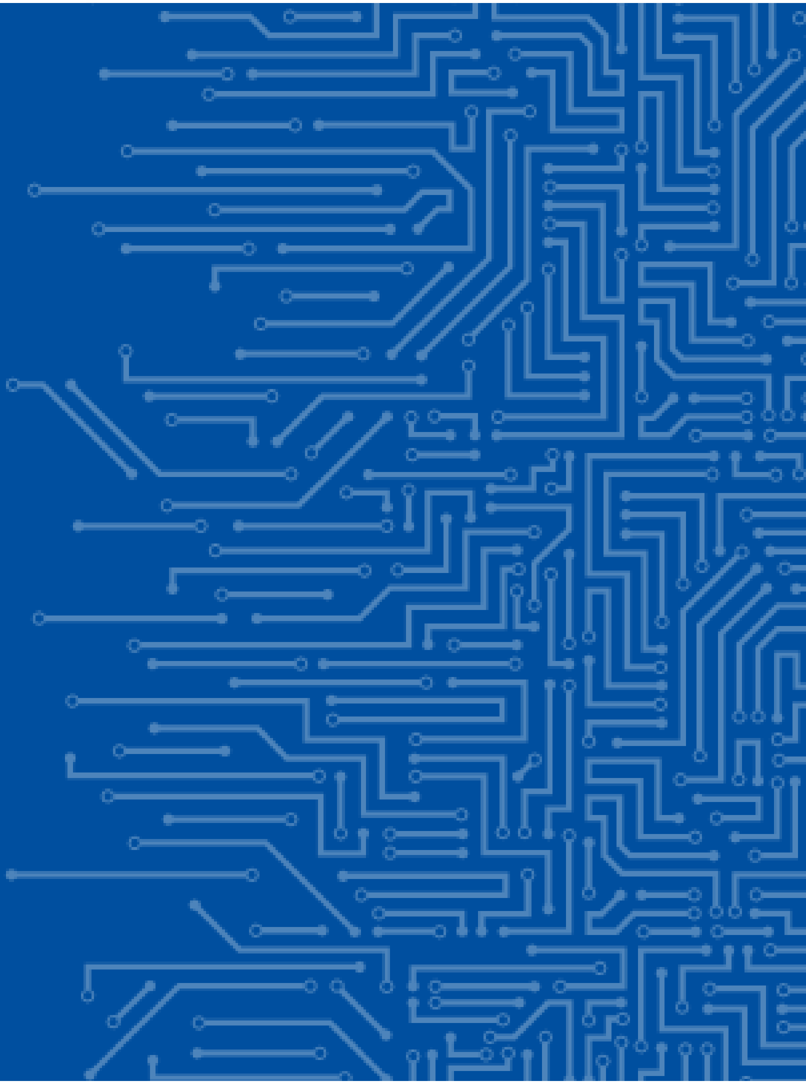
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

THE EUVD, EU CVD, AND THE CRA SRP

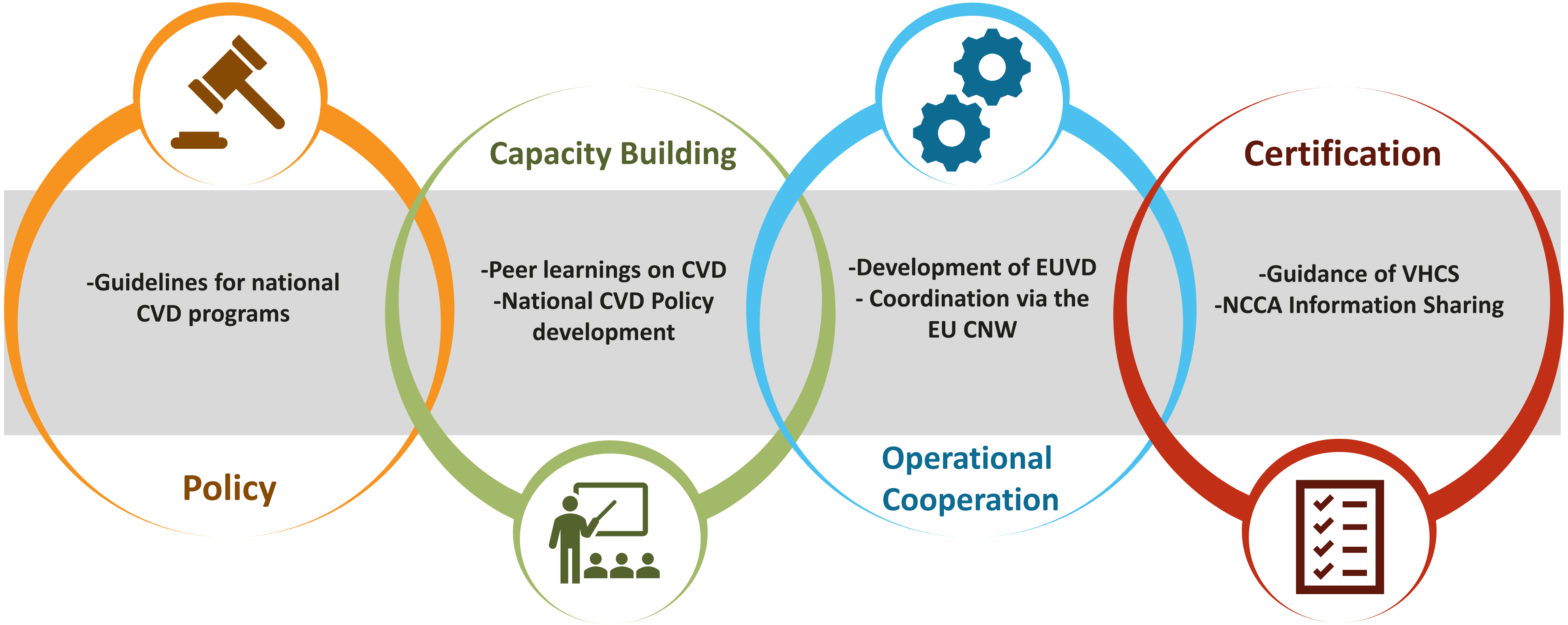
State of Play

CSAF Community Days
Johannes Clos

12 | 12 | 2024



SUPPORTING CVD AT ENISA



Policy

-Guidelines for national CVD programs

Capacity Building

-Peer learnings on CVD
-National CVD Policy development

Operational Cooperation

-Development of EUVD
- Coordination via the EU CNW

Certification

-Guidance of VHCS
-NCCA Information Sharing

STUDIES AND GUIDELINES

2021

CVD Policies in the EU

feeding into…

Stocktaking of status of CVD policies across the EU. Major concerns and obstacles in CVD development.

COORDINATED VULNERABILITY DISCLOSURE POLICIES IN THE EU

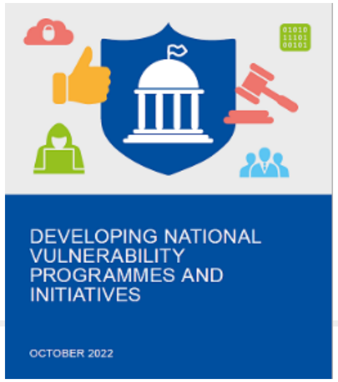
APRIL 2022

2022

CVD Challenges and Initiatives

feeding into…

Deep dive into the industry perspective on national CVD policies. Good practices to address legal, technical, and collaborative .



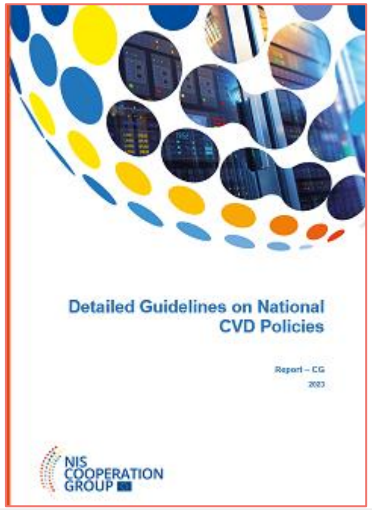
DEVELOPING NATIONAL VULNERABILITY PROGRAMMES AND INITIATIVES

OCTOBER 2022

2023

Detailed Guidelines on CVD Policies

Good practices from previous studies and MS experiences.

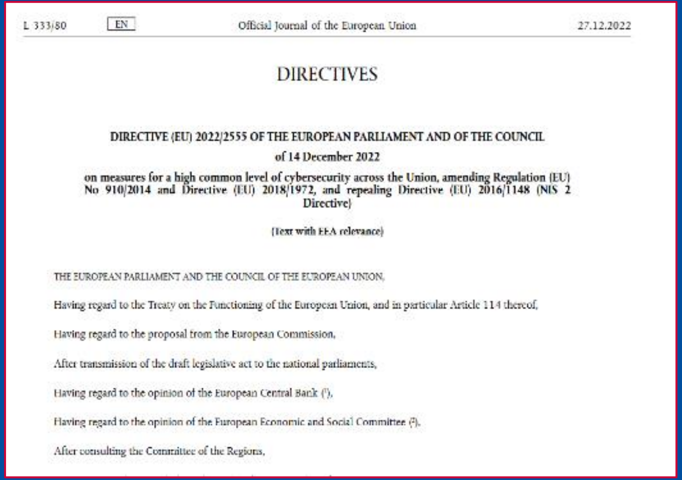


Detailed Guidelines on National CVD Policies

Report – CG

2023

NIS COOPERATION GROUP



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

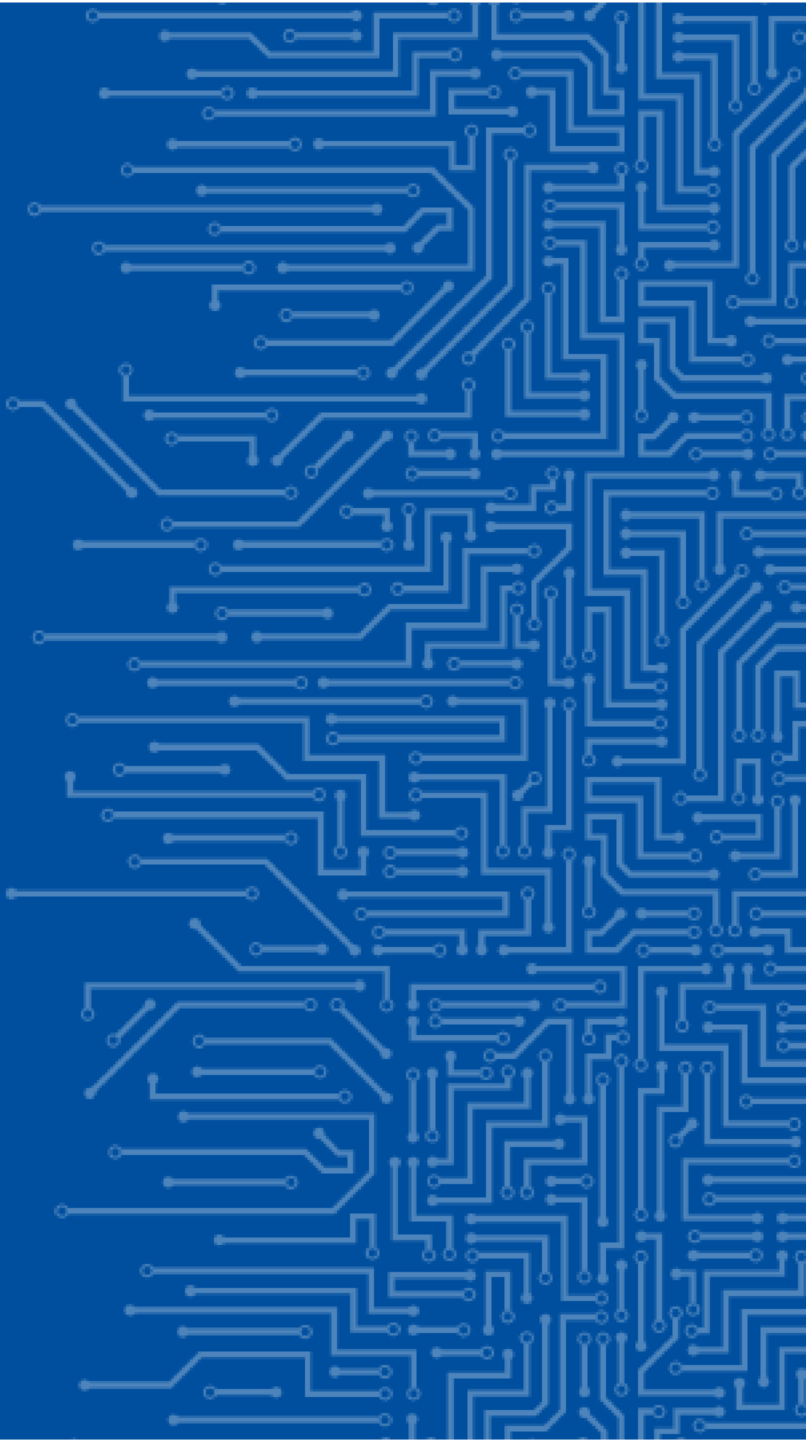
After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank [1],

Having regard to the opinion of the European Economic and Social Committee [2],

After consulting the Committee of the Regions,

NIS2 Directive

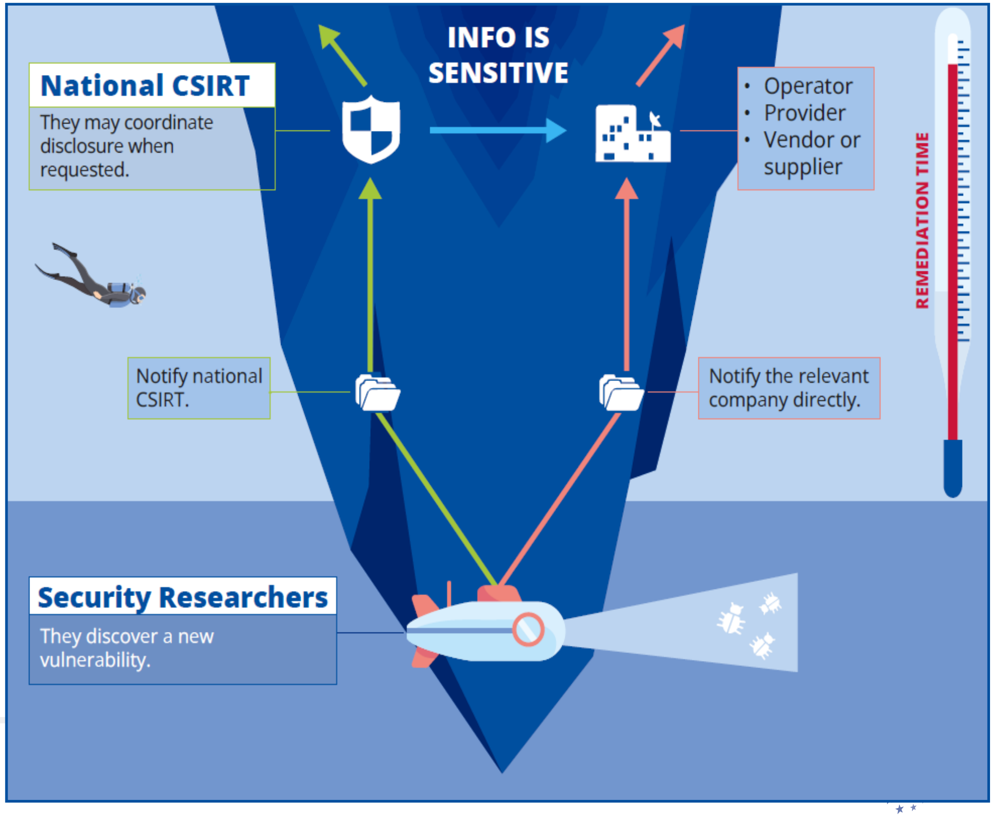


THE EUVD + EU CVD

EU VULNERABILITY DISCLOSURE

NIS2 Keypoints - Coordinated Disclosure by MS

- MS shall designate one of its CSIRTs as coordinator for coordinated vulnerability disclosure
  - trusted intermediary, facilitating the interaction between the entity reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services
- The coordinating CSIRT shall cooperate with other coordinators within the CSIRTs network



INFO IS SENSITIVE

National CSIRT

They may coordinate disclosure when requested.

- Operator
- Provider
- Vendor or supplier

Notify national CSIRT.

Notify the relevant company directly.

Security Researchers

They discover a new vulnerability.

CSIRTS > COORDINATED DISCLOSURE

State-of-play on CVD

An increasing number of MS and CERT-EU published CVD policies. Some EU Member States’ CSIRTs have national vulnerability registries in place.

Decision on CSIRT coordinator

Formal assignment of coordinating CSIRT by EU MS pending.

Level of interconnection among databases

‘Cross-referencing’ practices are relatively low. Limited and inconsistent content in terms of details, sources and references as well as lacking vulnerability IDs are a barrier to cross-referencing and data triangulation.

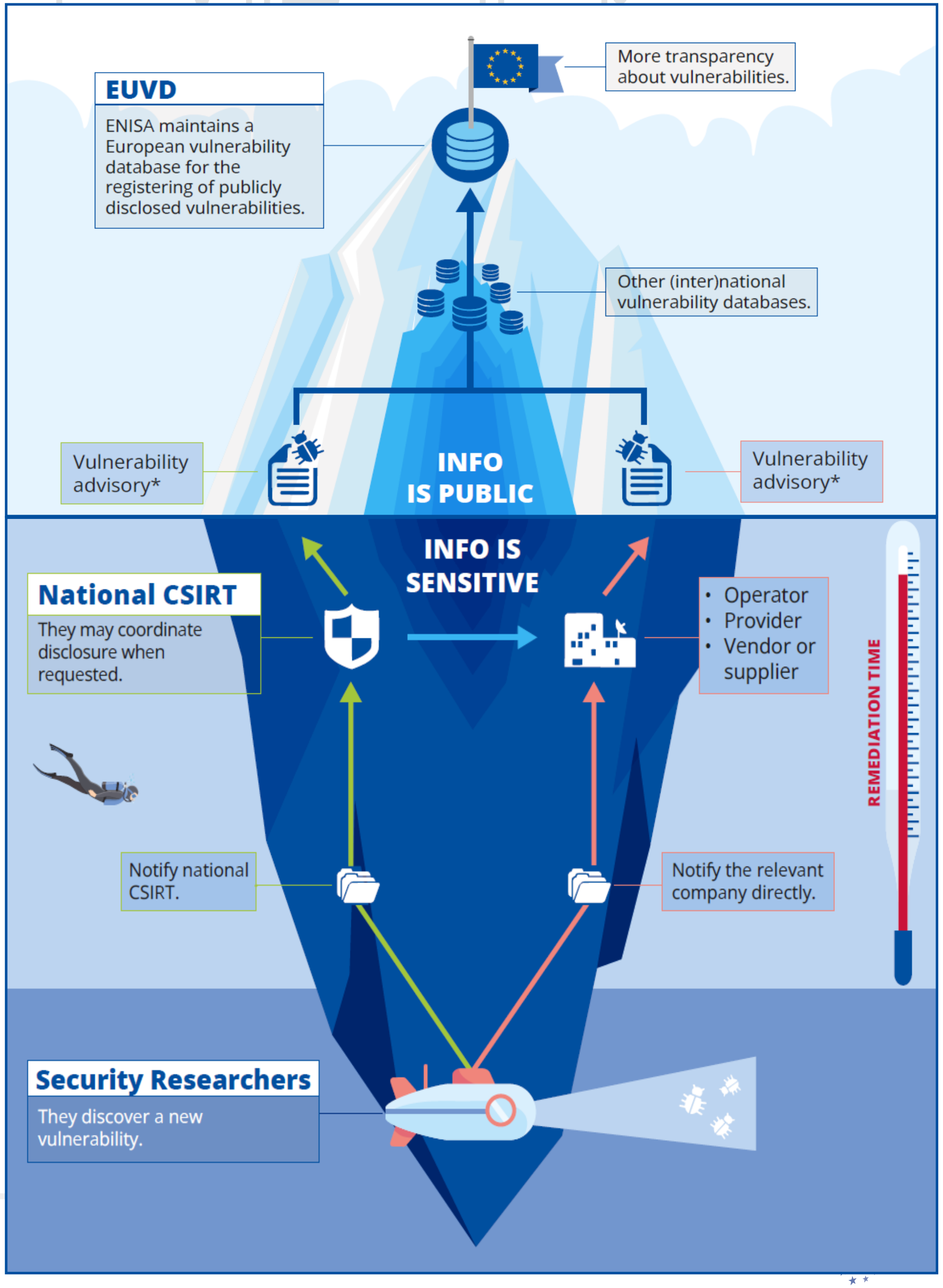
EU VULNERABILITY DATABASE

NIS2 Keypoints - EUVD & Registry service

- Publicly available

- Database entries need to include
  - Description of the vulnerability
  - Affected ICT service, severity, exploitability
  - Patch information and mitigation guidance

- Solution needs to build upon & utilize existing standards



EUVD

ENISA maintains a European vulnerability database for the registering of publicly disclosed vulnerabilities.

More transparency about vulnerabilities.

Other (inter)national vulnerability databases.

Vulnerability advisory*

Vulnerability advisory*

INFO IS PUBLIC

INFO IS SENSITIVE

National CSIRT

They may coordinate disclosure when requested.

- Operator
- Provider
- Vendor or supplier

REMEDIATION TIME

Notify national CSIRT.

Notify the relevant company directly.

Security Researchers

They discover a new vulnerability.

ENISA > SUPPORT & DISCLOSURE

State-of-play

Following an EUVD stakeholder feedback collection phase and an internal preparation exercise ENISA finalized onboarding procedure for becoming a vulnerability registry (CVE Numbering Authority)

CNA approach

Registry service will focus on vulnerabilities that are reported by regional researchers, coordinated and disclosed by European CSIRTs, and that are affecting European vendors

EUVD following a holistic approach

Level of interconnection among databases

Where available, external data sources will be included in order to increase data quality and coverage

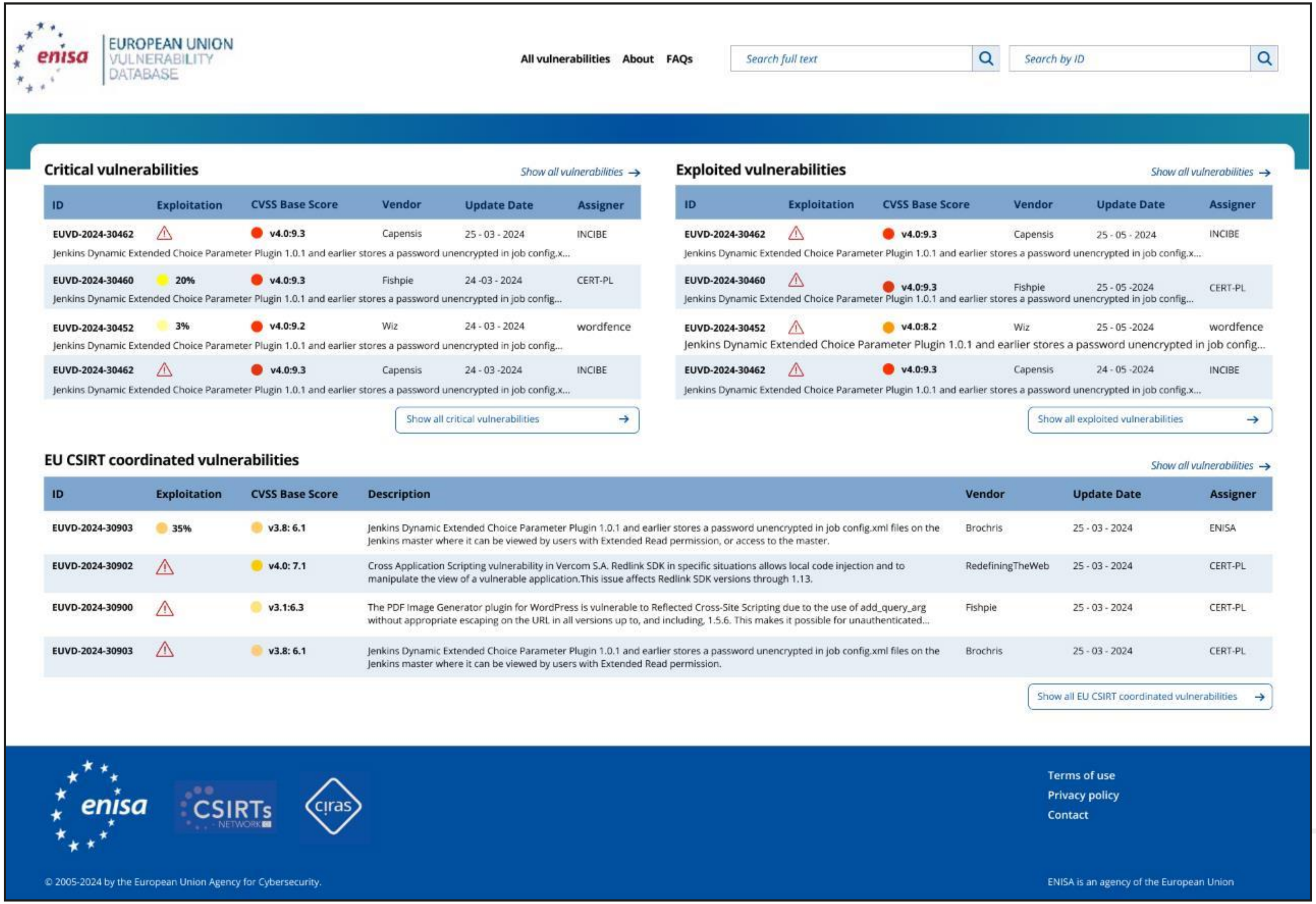
Level of interconnection among databases

Where available, external data sources will be included in order to increase data quality and coverage

Feeding the EUVD concept

- **Data synchronisation with existing databases** is practiced wherever possible by utilizing the OSS project **Vulnerability-Lookup** maintained by CIRCL.
- Builds upon **existing standards and systems** such as CVE, CVSS, EPSS, and highlights the severity and monitored exploitation of vulnerabilities.
- Available information relates to **impacted software versions** for being effectively usable.
- Utilizes **Common Security Advisory Framework** (currently as Aggregator) in order to collect vulnerability information and to make EUVD data available (trusted provider) in a standardized machine-readable format (as part of an upcoming enhancement).

VULNERABILITY DATABASE



EUROPEAN UNION VULNERABILITY DATABASE

Critical vulnerabilities

Show all vulnerabilities →

ID	Exploitation	CVSS Base Score	Vendor	Update Date	Assigner
EUVD-2024-30462	⚠	● v4.0:9.3	Capensis	25 - 03 - 2024	INCIBE
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.x...					
EUVD-2024-30460	● 20%	● v4.0:9.3	Fishpie	24 -03 - 2024	CERT-PL
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config...					
EUVD-2024-30452	● 3%	● v4.0:9.2	Wiz	24 - 03 - 2024	wordfence
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config...					
EUVD-2024-30462	⚠	● v4.0:9.3	Capensis	24 - 03 -2024	INCIBE
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.x...					

Show all critical vulnerabilities →

Exploited vulnerabilities

Show all vulnerabilities →

ID	Exploitation	CVSS Base Score	Vendor	Update Date	Assigner
EUVD-2024-30462	⚠	● v4.0:9.3	Capensis	25 - 05 - 2024	INCIBE
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.x...					
EUVD-2024-30460	⚠	● v4.0:9.3	Fishpie	25 - 05 -2024	CERT-PL
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config...					
EUVD-2024-30452	⚠	● v4.0:8.2	Wiz	25 - 05 -2024	wordfence
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config...					
EUVD-2024-30462	⚠	● v4.0:9.3	Capensis	24 - 05 -2024	INCIBE
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.x...					

Show all exploited vulnerabilities →

EU CSIRT coordinated vulnerabilities

Show all vulnerabilities →

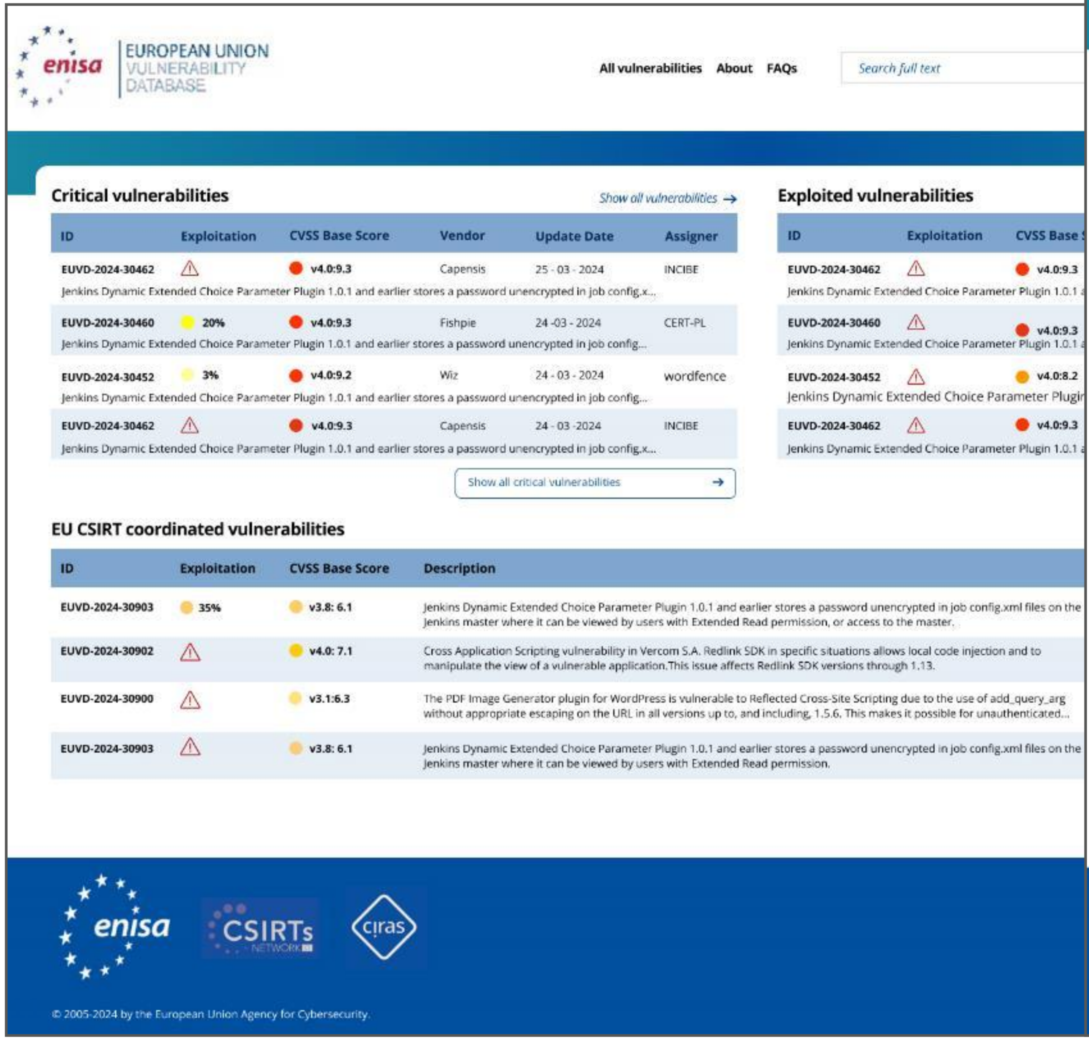
ID	Exploitation	CVSS Base Score	Description	Vendor	Update Date	Assigner
EUVD-2024-30903	● 35%	● v3.8: 6.1	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master.	Brochris	25 - 03 - 2024	ENISA
EUVD-2024-30902	⚠	● v4.0: 7.1	Cross Application Scripting vulnerability in Vercom S.A. Redlink SDK in specific situations allows local code injection and to manipulate the view of a vulnerable application.This issue affects Redlink SDK versions through 1.13.	RedefiningTheWeb	25 - 03 - 2024	CERT-PL
EUVD-2024-30900	⚠	● v3.1:6.3	The PDF Image Generator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated...	Fishpie	25 - 03 - 2024	CERT-PL
EUVD-2024-30903	⚠	● v3.8: 6.1	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission.	Brochris	25 - 03 - 2024	CERT-PL

Show all EU CSIRT coordinated vulnerabilities →

© 2005-2024 by the European Union Agency for Cybersecurity.

ENISA is an agency of the European Union

VULNERABILITY DATABASE



Critical vulnerabilities

Show all vulnerabilities →

ID	Exploitation	CVSS Base Score	Vendor	Update Date	Assigner
EUVD-2024-30462	⚠	● v4.0:9.3	Capensis	25 - 03 - 2024	INCIBE
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.x...					
EUVD-2024-30460	● 20%	● v4.0:9.3	Fishpie	24 -03 - 2024	CERT-PL
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config...					
EUVD-2024-30452	● 3%	● v4.0:9.2	Wiz	24 - 03 - 2024	wordfence
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config...					
EUVD-2024-30462	⚠	● v4.0:9.3	Capensis	24 - 03 -2024	INCIBE
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.x...					

Show all critical vulnerabilities →

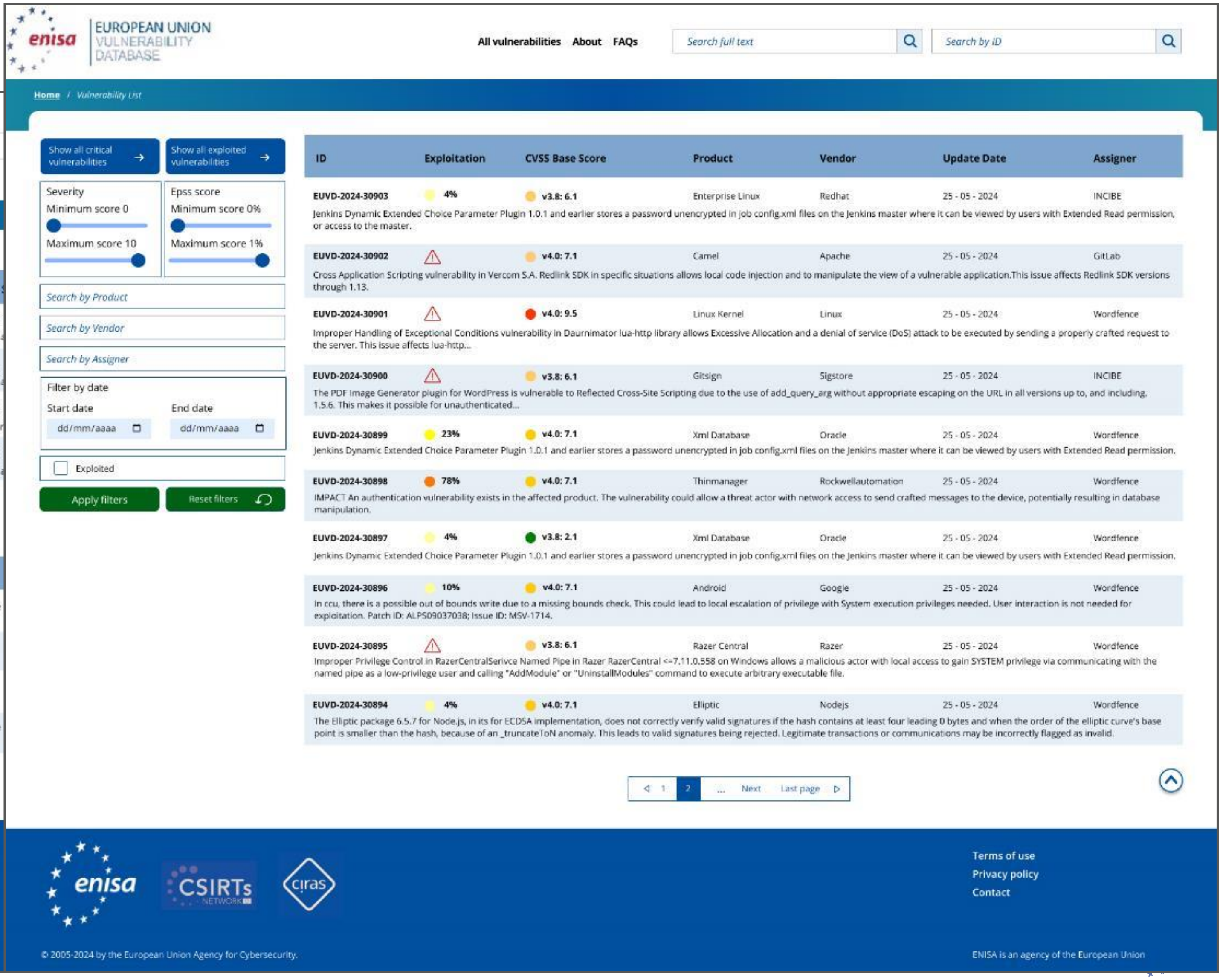
Exploited vulnerabilities

ID	Exploitation	CVSS Base S
EUVD-2024-30462	⚠	● v4.0:9.3
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 a		
EUVD-2024-30460	⚠	● v4.0:9.3
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 a		
EUVD-2024-30452	⚠	● v4.0:8.2
Jenkins Dynamic Extended Choice Parameter Plugir		
EUVD-2024-30462	⚠	● v4.0:9.3
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 a		

EU CSIRT coordinated vulnerabilities

ID	Exploitation	CVSS Base Score	Description
EUVD-2024-30903	● 35%	● v3.8: 6.1	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master.
EUVD-2024-30902	⚠	● v4.0: 7.1	Cross Application Scripting vulnerability in Vercom S.A. Redlink SDK in specific situations allows local code injection and to manipulate the view of a vulnerable application.This issue affects Redlink SDK versions through 1.13.
EUVD-2024-30900	⚠	● v3.1:6.3	The PDF Image Generator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated...
EUVD-2024-30903	⚠	● v3.8: 6.1	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission.

© 2005-2024 by the European Union Agency for Cybersecurity.


enisa
EUROPEAN UNION
VULNERABILITY
DATABASE
All vulnerabilities
About
FAQs
Search full text
Search by ID
Home / Vulnerability List
Show all critical vulnerabilities →
Show all exploited vulnerabilities →

Severity
Minimum score 0
Maximum score 10

Epss score
Minimum score 0%
Maximum score 1%

Search by Product

Search by Vendor

Search by Assigner

Filter by date
Start date dd/mm/aaaa
End date dd/mm/aaaa

☐ Exploited

Apply filters

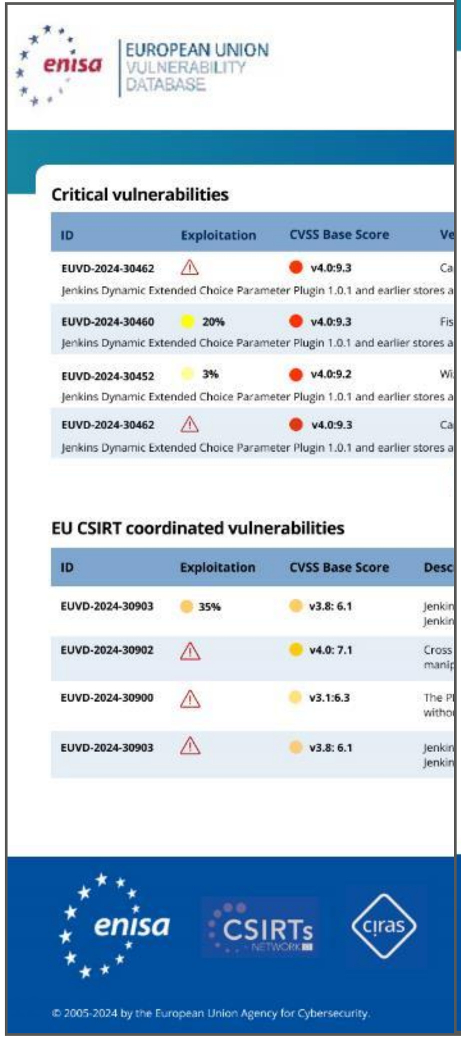
Reset filters

ID	Exploitation	CVSS Base Score	Product	Vendor	Update Date	Assigner
EUVD-2024-30903	● 4%	● v3.8: 6.1	Enterprise Linux	Redhat	25 - 05 - 2024	INCIBE
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master.						
EUVD-2024-30902	⚠	● v4.0: 7.1	Camel	Apache	25 - 05 - 2024	GitLab
Cross Application Scripting vulnerability in Vercom S.A. Redlink SDK in specific situations allows local code injection and to manipulate the view of a vulnerable application.This issue affects Redlink SDK versions through 1.13.						
EUVD-2024-30901	⚠	● v4.0: 9.5	Linux Kernel	Linux	25 - 05 - 2024	Wordfence
Improper Handling of Exceptional Conditions vulnerability in Daurnimator lua-http library allows Excessive Allocation and a denial of service (DoS) attack to be executed by sending a properly crafted request to the server. This issue affects lua-http...						
EUVD-2024-30900	⚠	● v3.8: 6.1	Gitsign	Sigstore	25 - 05 - 2024	INCIBE
The PDF Image Generator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated...						
EUVD-2024-30899	● 23%	● v4.0: 7.1	Xml Database	Oracle	25 - 05 - 2024	Wordfence
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission.						
EUVD-2024-30898	● 78%	● v4.0: 7.1	Thinmanager	Rockwellautomation	25 - 05 - 2024	Wordfence
IMPACT An authentication vulnerability exists in the affected product. The vulnerability could allow a threat actor with network access to send crafted messages to the device, potentially resulting in database manipulation.						
EUVD-2024-30897	● 4%	● v3.8: 2.1	Xml Database	Oracle	25 - 05 - 2024	Wordfence
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission.						
EUVD-2024-30896	● 10%	● v4.0: 7.1	Android	Google	25 - 05 - 2024	Wordfence
In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09037038; Issue ID: MSV-1714.						
EUVD-2024-30895	⚠	● v3.8: 6.1	Razer Central	Razer	25 - 05 - 2024	Wordfence
Improper Privilege Control in RazerCentralSerivce Named Pipe in Razer RazerCentral <=7.11.0.558 on Windows allows a malicious actor with local access to gain SYSTEM privilege via communicating with the named pipe as a low-privilege user and calling "AddModule" or "UninstallModules" command to execute arbitrary executable file.						
EUVD-2024-30894	● 4%	● v4.0: 7.1	Elliptic	Nodejs	25 - 05 - 2024	Wordfence
The Elliptic package 6.5.7 for Node.js, in its for ECDSA implementation, does not correctly verify valid signatures if the hash contains at least four leading 0 bytes and when the order of the elliptic curve's base point is smaller than the hash, because of an _truncateToN anomaly. This leads to valid signatures being rejected. Legitimate transactions or communications may be incorrectly flagged as invalid.						

© 2005-2024 by the European Union Agency for Cybersecurity.

ENISA is an agency of the European Union

VULNERABILITY DATABASE



EUROPEAN UNION VULNERABILITY DATABASE

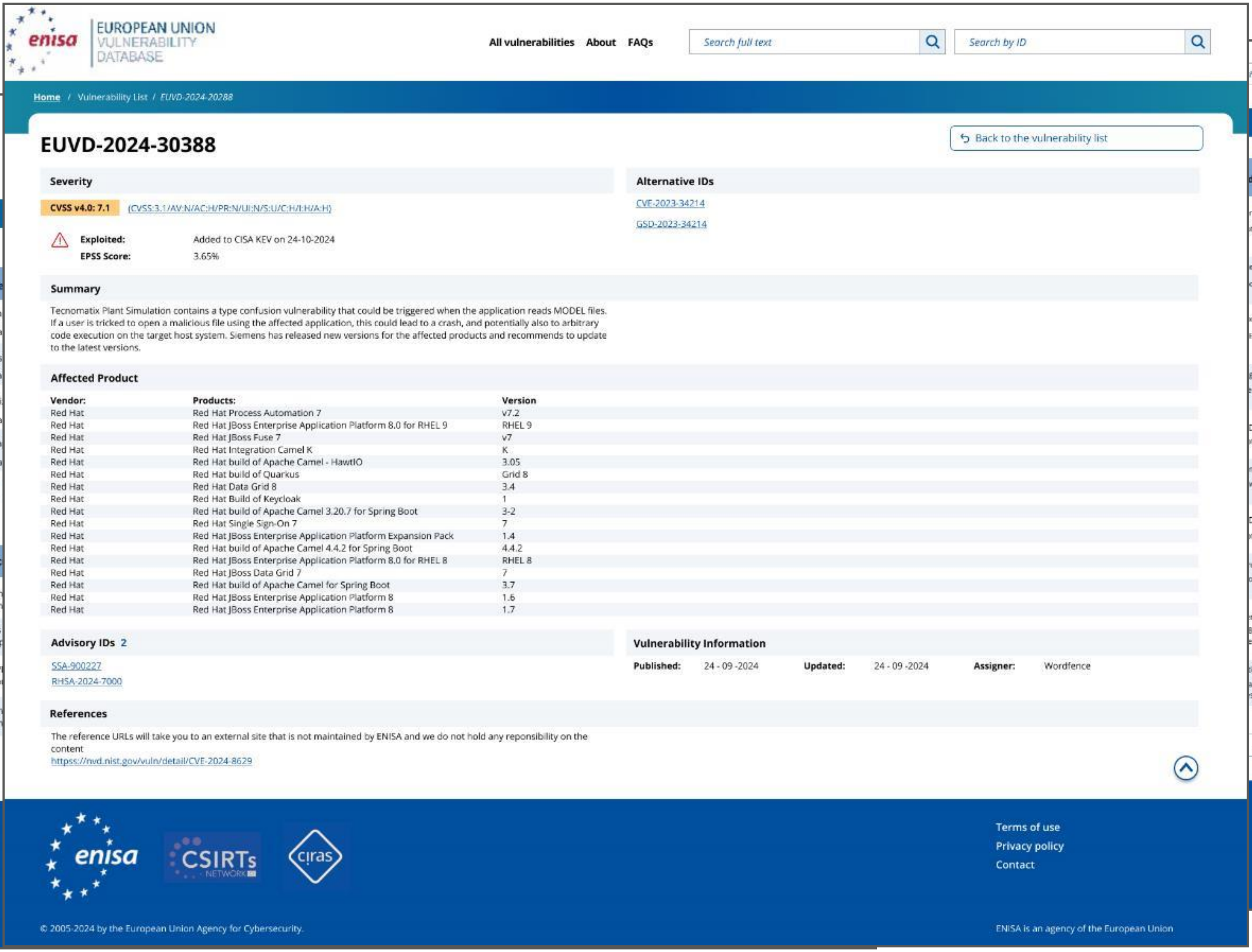
Critical vulnerabilities

ID	Exploitation	CVSS Base Score	Ve
EUVD-2024-30462	⚠	● v4.0:9.3	Ca
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a			
EUVD-2024-30460	● 20%	● v4.0:9.3	Fis
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a			
EUVD-2024-30452	● 3%	● v4.0:9.2	Wi
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a			
EUVD-2024-30462	⚠	● v4.0:9.3	Ca
Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a			

EU CSIRT coordinated vulnerabilities

ID	Exploitation	CVSS Base Score	Desc
EUVD-2024-30903	● 35%	● v3.8: 6.1	Jenkin Jenkin
EUVD-2024-30902	⚠	● v4.0: 7.1	Cross manip
EUVD-2024-30900	⚠	● v3.1:6.3	The Pl withou
EUVD-2024-30903	⚠	● v3.8: 6.1	Jenkin Jenkin

© 2005-2024 by the European Union Agency for Cybersecurity.



EUROPEAN UNION VULNERABILITY DATABASE

All vulnerabilities About FAQs

Search full text

Search by ID

Home / Vulnerability List / EUVD-2024-20288

EUVD-2024-30388

Back to the vulnerability list

Severity

CVSS v4.0: 7.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

⚠ **Exploited:** Added to CISA KEV on 24-10-2024

EPSS Score: 3.65%

Alternative IDs

CVE-2023-34214

GSD-2023-34214

Summary

Tecnomatix Plant Simulation contains a type confusion vulnerability that could be triggered when the application reads MODEL files. If a user is tricked to open a malicious file using the affected application, this could lead to a crash, and potentially also to arbitrary code execution on the target host system. Siemens has released new versions for the affected products and recommends to update to the latest versions.

Affected Product

Vendor:	Products:	Version
Red Hat	Red Hat Process Automation 7	v7.2
Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 9	RHEL 9
Red Hat	Red Hat JBoss Fuse 7	v7
Red Hat	Red Hat Integration Camel K	K
Red Hat	Red Hat build of Apache Camel - HawtIO	3.05
Red Hat	Red Hat build of Quarkus	Grid 8
Red Hat	Red Hat Data Grid 8	3.4
Red Hat	Red Hat Build of Keycloak	1
Red Hat	Red Hat build of Apache Camel 3.20.7 for Spring Boot	3-2
Red Hat	Red Hat Single Sign-On 7	7
Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	1.4
Red Hat	Red Hat build of Apache Camel 4.4.2 for Spring Boot	4.4.2
Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 8	RHEL 8
Red Hat	Red Hat JBoss Data Grid 7	7
Red Hat	Red Hat build of Apache Camel for Spring Boot	3.7
Red Hat	Red Hat JBoss Enterprise Application Platform 8	1.6
Red Hat	Red Hat JBoss Enterprise Application Platform 8	1.7

Advisory IDs 2

SSA-900227

RHSA-2024-7000

Vulnerability Information

Published: 24 - 09 -2024 **Updated:** 24 - 09 -2024 **Assigner:** Wordfence

References

The reference URLs will take you to an external site that is not maintained by ENISA and we do not hold any reponsibility on the content

https://nvd.nist.gov/vuln/detail/CVE-2024-8629

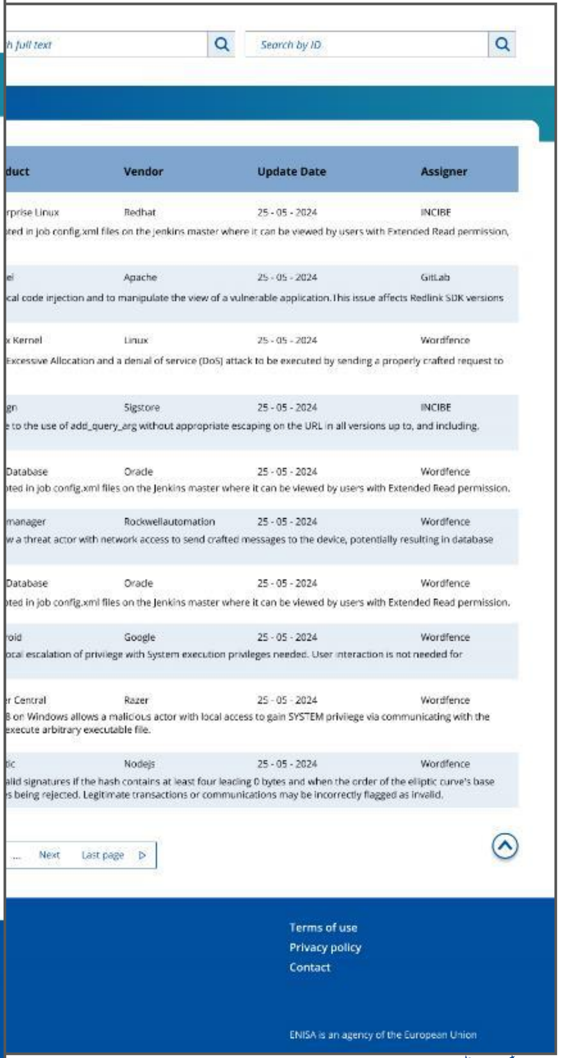
Terms of use

Privacy policy

Contact

© 2005-2024 by the European Union Agency for Cybersecurity.

ENISA is an agency of the European Union



Search full text

Search by ID

duct	Vendor	Update Date	Assigner
rprise Linux	Redhat	25 - 05 - 2024	INCIBE
ted in job config.xml files on the jenkins master where it can be viewed by users with Extended Read permission,			
el	Apache	25 - 05 - 2024	GitLab
cal code injection and to manipulate the view of a vulnerable application. This issue affects Redlink SDK versions			
x Kernel	Linux	25 - 05 - 2024	Wordfence
Excessive Allocation and a denial of service (DoS) attack to be executed by sending a properly crafted request to			
gn	Sigstore	25 - 05 - 2024	INCIBE
e to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including.			
Database	Oracle	25 - 05 - 2024	Wordfence
ted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission.			
manager	Rockwellautomation	25 - 05 - 2024	Wordfence
w a threat actor with network access to send crafted messages to the device, potentially resulting in database			
Database	Oracle	25 - 05 - 2024	Wordfence
ted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission.			
roid	Google	25 - 05 - 2024	Wordfence
ocal escalation of privilege with System execution privileges needed. User interaction is not needed for			
r Central	Razer	25 - 05 - 2024	Wordfence
8 on Windows allows a malicious actor with local access to gain SYSTEM privilege via communicating with the execute arbitrary executable file.			
tic	Nodejs	25 - 05 - 2024	Wordfence
alid signatures if the hash contains at least four leading 0 bytes and when the order of the elliptic curve's base s being rejected. Legitimate transactions or communications may be incorrectly flagged as invalid.			

... Next Last page ▷

Terms of use

Privacy policy

Contact

ENISA is an agency of the European Union

European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2024)0130

Cyber Resilience Act

European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

(Ordinary legislative procedure: first reading)

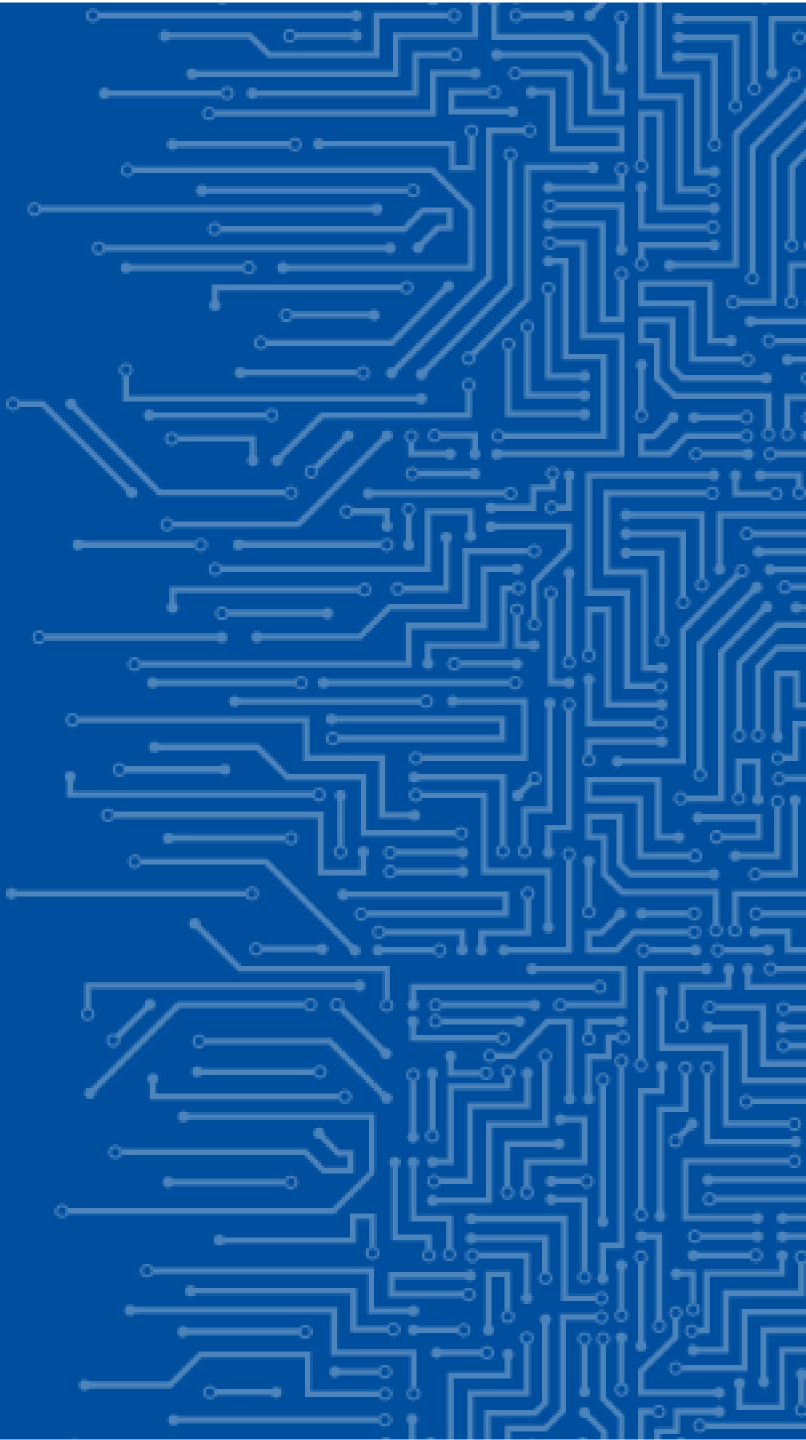
The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2022)0454),

– having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0308/2022),

Cyber Resilience Act

THE CRA SRP



REPORTING OBLIGATION [1]

	24 hrs.	72 hrs.	14 days	1 month
AEV [2]	• Early notification • Member States where product is available	• Impacted product(s) • Nature of the vulnerability • Initial Assessment • Corrective/mitigating actions	• Detailed description, severity and impact • Info on malicious actors • Security updates/corrective measures	
Incidents [3]	• Early notification • Whether is suspected caused by malicious act • Member States where product is available	• Nature of the incident • Initial Assessment • Corrective/mitigating actions		• Detailed description, severity and impact • Type of threat or root cause • Ongoing mitigation

[1] As defined by the regulation [https://eur-lex.europa.eu/eli/reg/2024/2847/oj]

[2] Actively Exploited Vulnerabilities

[3] Incidents having an impact on the security of the product with digital elements

SRP IMPLEMENTATION PLAN AND BENEFITS

Implementation Planning

- Stakeholder consultation
- Resources allocated (Finance and Human)
- Draw of High Level Design and specification
- Tender launch by early 2025
- Implementation and deployment
- Operational by July 26

Expected Benefit

- Contribute to Common Situational awareness and enable faster response at EU Level
- Create a safe channel for Responder to Vendor information exchange
- Increase maturity on PSIRT process in the EU internal market
- Provide opportunity for consolidation of mandatory reporting for Cyber

THE EUVD AND THE CRA SRP

Information exchange standard will likely be CSAF

- industry accepted language created for exchanging security related advisories.
- allows participants to automate the creation, consumption and exchange of security vulnerability information and remediation.
- covers both types of information that the solution will need to handle, i.e. vulnerability and incident reports.
- supports different “profiles” (customisations to cover reporting entity and/or use-case specific needs). Relevant profiles shall be defined and published through the platform making potential integrators with the platform aware of the supported data format and schema.

THE EUVD AND THE CRA SRP

After a security update or another form of corrective or mitigating measure is available, ENISA shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified to the European vulnerability database established

- Manufacturers should exercise due diligence. The appropriate level depends on the nature and the level of cybersecurity risk associated with a given component by verifying that a component is free from vulnerabilities registered in the European vulnerability database or other publicly accessible vulnerability DBs.

- ENISA [should] have an adequate overview of such vulnerabilities and are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities as well as to ensure the effective functioning of market surveillance authorities.

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

✉ info@enisa.europa.eu

🌐 www.enisa.europa.eu