TELEMETRY

Policy brief on EUVD

A European Vulnerability Database with API Access

Funded by the European Union

This project is funded by the European Union under grant agreement ID 101119747. The information and views set out in this document are those of the TELEMETRY Consortium only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

Contents

Introduction

The European Union Agency for Cybersecurity (ENISA) launched the European Union Vulnerability Database (EUVD) in April 2025 as part of the operationalization of cybersecurity requirements established under the NIS2 Directive (Directive (EU) 2022/2555). The EUVD is designed to serve as the EU's primary repository for aggregated vulnerability intelligence, vendor advisories, national CSIRT alerts, CVE and CVSS scores, EPSS exploitation probability metrics, and exploitation status derived from the CISA Known Exploited Vulnerabilities (KEV) catalogue.

The EUVD's importance extends beyond its function as a technical database. It is intended to reduce dependency on non-EU vulnerability infrastructures and to support EU-wide regulatory and operational needs, including those emerging under the Cyber Resilience Act (CRA) for products with digital elements.

From a governance perspective, the EUVD is a NIS2-mandated capability intended to support coordinated vulnerability disclosure and strengthen information sharing across Member States, including via national CSIRTs. It is also related to the CRA: while the CRA foresees a Single Reporting Platform (SRP) for regulatory reporting[1], the EUVD provides broader vulnerability intelligence that can inform compliance, supervision, and risk management. As a Common Vulnerability and Exposure (CVE) Numbering Authority (CNA), ENISA is authorised to assign CVE Identifiers (CVE IDs) and to publish CVE Records for vulnerabilities discovered by or reported to EU CSIRTs, in line with their dedicated coordinator roles since January 2024. As Root CNA, ENISA is now expanding its role within the CVE program leveraging the EUVD.

The EUVD responds to two operational targets: resilience concerns created by reliance on US-based vulnerability infrastructure, and the shift toward automation in vulnerability management and software supply-chain assurance. In fact, both Cyber Threat Intelligence and SBOM-based dependency tracking and controls require stable, machine-readable APIs with sufficient metadata to match affected products and versions at scale.

This Policy brief provides a short technical assessment of the EUVD's public REST API, accessible at https://euvd.enisa.europa.eu/apidoc, with the dual aim of evaluating its current capabilities for programmatic integration and identifying developer-oriented improvements that could enhance its utility for security practitioners, tool developers, and regulated entities operating under EU cybersecurity law.

The availability of a robust, high-performance Application Programming Interface (API) is vital for the integration of the EUVD into modern cybersecurity and Cyber Threat Intelligence (CTI) ecosystems. To move beyond manual human-based processes, the database must provide seamless, machine-readable access to vulnerability data, enabling automation to ingest and correlate threat feeds in real-time, and facilitating the effective integration of this valuable

[1] The European Vulnerability Database (EUVD) is not the same as the Single Reporting Platform (SRP). While both are initiatives developed by ENISA (European Union Agency for Cybersecurity) to enhance cybersecurity under EU regulations, they serve different, albeit complementary, functions. The Single Reporting Platform (SRP) under the EU Cyber Resilience Act (CRA) has faced several criticisms and concerns from industry experts and cybersecurity researchers; that criticism is outside the scope of this document, as it is focused only on the EUVD.

asset into more advanced approaches, such as those based on agentic AI. A sound API architecture is a technical need for reducing the window of exposure between vulnerability discovery and remediation, ensuring that EU defence mechanisms can scale to meet the velocity of contemporary cyber threats.

1 Policy and Governance context

Operationally, the EUVD is intended to facilitate voluntary reporting and registration by entities and their suppliers, while enabling competent authorities, most notably national Computer Security Incident Response Teams (CSIRTs), to contribute vulnerability information and support mitigation by end users. This design implies that the EUVD's long-term value is not only technical (data aggregation) but also procedural, as it can support coordinated disclosure workflows within EU governance.

In the wider EU regulatory ecosystem, the EUVD's relevance is amplified by the CRA's emphasis on vulnerability handling for products with digital elements. While the CRA's SRP[2] serves a distinct reporting purpose, both initiatives depend on high-integrity, timely vulnerability information for enforcement, supervision, and market-wide risk management. Sustained alignment with the CVE identifier space remains important to minimise fragmentation and preserve interoperability for vendors and toolchains.

The resilience rationale has a concrete implication: European operators need a vulnerability data source whose availability, timeliness, and governance are predictable even when upstream programmes experience disruption, because dependence on external vulnerability infrastructures introduces systemic risk for EU cybersecurity operations[3]. As a result, the EUVD should be evaluated not only by feature completeness, but also by continuity of service and dependable publication and update behaviour at EU scale.

Similarly, the automation rationale translates into specific API expectations: machine-readable outputs suitable for ingestion, sufficient metadata for affected-product matching, and throughput that supports continuous monitoring rather than occasional manual lookup. These expectations are increasingly driven by SBOM-oriented practices and pipeline-integrated vulnerability management.

IoT and cyber-physical implementations serve as real-time vulnerability indicators for Class II products listed in Annex III of the CRA that contain digital elements. When structured as machine-readable data (asset identifiers, timestamps, severity levels and component-level attribution). This highlights that the value of the EUVD as a regulatory compliance infrastructure depends not only on the comprehensiveness of the dataset, but also on its ability to serve as a stable correlation reference point for telemetry channels, a function that imposes specific requirements regarding the richness of API metadata and the accuracy of product mapping.

In this context, possible gaps in the API dataset, missing bulk and delta mechanisms, and incomplete product-matching metadata are not just usability issues: they limit the EUVD's ability to function as dependable infrastructure for large-scale automation and compliance-oriented processes.

Table 1compares the EUVD with the MITRE CVE and NIST NVD.

[3] NIST recently announced it will only enrich CVEs that appear in a federal catalog of exploited vulnerabilities (CISA).

Table 1: EUVD vs. MITRE CVE vs. NIST NVD: Key Differences

Aspect	EUVD	MITRE CVE	NIST NVD
Operator	ENISA (European Union Agency for Cybersecurity)	MITRE Corporation (USA)	NIST (USA)
Purpose	Supports NIS2 Directive; improves EU vulnerability coordination	Global vulnerability identification and cataloguing	U.S. national repository
ID Format	Assigns EUVD-specific IDs, with cross-references to CVEs	Assigns CVE IDs (for example, CVE-2025-XXXX)	CVE-centric, support CPE and CWE
Stakeholder Input	Aggregates input from EU CSIRTs, vendors, and operators	Primarily vendor submissions and CVE Numbering Authorities (CNA) partners	Enriches CVE data with additional analysis from NIST and external feeds
Mitigation Guidance	May provide actionable mitigations, exploitation status, and practical remediation info	Basic description with links; less focused on real-time mitigation status	Includes references and sometimes mitigation guidance
Regulatory Context	Aligned with NIS2 to support EU-wide cybersecurity governance	No binding alignment with regulatory mandates	U.S federal standards
Access	Public and free	Public and free	Public and free
API	Yes, limited	YES, limited	Yes, widely used

2 API Architecture and Data model evaluation

The EUVD API is a stateless REST interface that accepts HTTP GET requests and returns responses in JSON format. Authentication is not required, enabling consumers to begin querying the database without registration or credential management.

The API specification is published in OpenAPI format, which affords a degree of interoperability not always present in public government APIs. The availability of a machine-readable specification has already enabled the community-driven generation of client libraries in multiple programming languages.

The API exposes the principal endpoints listed in Table 2.

Table 2: EUVD API End Points

Endpoint	Description
/api/search	Primary search endpoint with multi-dimensional filtering (vendor, product, CVSS score range, EPSS range, exploitation status, date range, assigner, free text). Supports pagination with a maximum page size of 100 records.
/api/enisaid	Retrieves a single vulnerability record by its EUVD identifier (e.g., EUVD-2025-4893).
/api/advisory	Retrieves a vendor or CSIRT advisory by its identifier.
/api/lastvulnerabilities	Returns the most recently published vulnerabilities. Hard-limited to 8 records.
/api/criticalvulnerabilities	Alias for a search with CVSS score ≥ 9. Hard-limited to 8 records.
/api/exploitedvulnerabilities	Returns vulnerabilities with confirmed exploitation status. Hard-limited to 8 records.
/api/dump/cve-euvd-mapping	Full dataset (CSV with columns: euvd_id, cve_id). Contains only records linked to published CVEs. Updated daily at 07:00 UTC.
/api/kev/dump	Full dataset (JSON). Consolidated Known Exploited Vulnerabilities from CISA KEV and ENISA EU KEV sources.

Each vulnerability record returned by the search endpoint contains the following fields: a unique EUVD identifier, a textual description, publication and update timestamps, a CVSS base score (usually the version 4) with version and vector string, newline-delimited reference URLs, CVE aliases, the assigning CNA, an EPSS score, and arrays of associated product and vendor identifiers. The total count of records matching the query is returned as a top-level field, enabling consumers to implement paginated retrieval. The EUVD API offers high accessibility through an unauthenticated, OpenAPI-compliant architecture featuring multi-source

aggregation and advanced filtering, including probabilistic risk signals like EPSS, which significantly lowers the barrier for automated research and small-scale integration.

However, its current operational utility is constrained by critical data gaps, specifically the absence of CWE/CPE metadata, and CVSS Source Attribution, and the omission of over 15,000 CVE records from search results[4], alongside performance bottlenecks such as non-standard date formatting, restricted response sizes on convenience endpoints, and the lack of incremental synchronization support. These technical gaps and limitations currently limit the platform's suitability for high-fidelity, automated compliance workflows and bulk industrial ingestion.

Furthermore, the current data structure lacks the explicit semantic enrichment necessary for advanced AI automation, which requires unambiguous context to differentiate between illustrative examples and universally applicable data points, thus limiting the precision of AI-driven threat intelligence, risk assessment and automated translation to tools like intrusion detection systems.

[4] This gap seems to be reduced over time.

3 Improvements for a future EUVD

Table 3 lists recommended extensions to the EUVD API.

Table 3: EUVD API End Points suggested extensions

Focus Area	Recommendation	Rationale & Impact
Data Standardization	Adopt ISO 8601 Timestamps	Replace human-readable dates with UTC-compliant strings (e.g., 2025-04-15T20:30:58Z) to eliminate locale-dependent parsing errors in multizone EU environments.
Asset Mapping	Integrate CWE and CPE Fields	Include structured arrays for Common Weakness Enumeration and Common Platform Enumeration to enable automated SBOM matching and root-cause analysis for CRA compliance.
Sync Efficiency	Implement Delta Synchronization	Add an updated Since parameter to allow integrators to retrieve only modified records, reducing bandwidth and processing overhead for SOC toolchains.
Endpoint Utility	Increase Convenience Response Limits	Replace the static eight-record cap on specialized endpoints with configurable parameters (e.g., up to 100 records) to support daily batch monitoring.
Risk Provenance	Add CVSS Source Attribution	Explicitly identify the scoring authority (e.g., ENISA, NVD, or Vendor) to allow consumers to calibrate risk based on the data's origin.
Real-time Alerting	Support Webhooks/Push Notifications	Enable event-driven alerts for critical or exploited vulnerabilities to minimize latency in incident response and SIEM integrations.
Data Enrichment for AI Automation	Define a well-known namespace and include an example field	Improve the utility for AI automated systems by providing clearer differentiation and avoid confuse illustrative names or values with definitive, generic truths, leading to misinterpretations or incorrect outputs.

4 Conclusion

The establishment of the European Union Vulnerability Database (EUVD) represents a significant shift toward European digital sovereignty by providing a regional alternative to non-EU repositories, such as the US-based National Vulnerability Database (NVD). By reducing systemic dependency on foreign entities for threat intelligence, the EUVD ensures that the classification and disclosure of cyber risks remain aligned with European strategic interests and the specific security requirements of the Union's digital single market.

As a central pillar of the EU's evolving cybersecurity architecture, the EUVD creates critical operational synergies with the NIS2 Directive and the forthcoming Cyber Resilience Act (CRA). While the EUVD enhances regional resilience through specialized dashboards and exploit prediction scoring, its long-term efficacy depends on rigorous technical interoperability with global standards, including also the Common Weakness Enumeration (CWE) system and Common Platform Enumeration (CPE). To support automated security workflows and high-volume research, EUVD should prioritize API performance, the consistency of metadata, and the integration of open-source software vulnerabilities to prevent data fragmentation.

The current EUVD API, an essential feature for Cyber Threat Intelligence architectures, can be viewed as an early iteration of an EU-operated public vulnerability data service. Its open access model, expressive search interface, and multi-source aggregation provide a sound technical foundation for programmatic vulnerability intelligence workflows. However, several limitations, most notably limited enrichment, incomplete CVE coverage in bulk search results, the absence of CWE and CPE metadata, non-standard date formatting, and performance constraints under bulk retrieval, currently constrain its utility as a production-grade alternative to established databases such as the NIST NVD: EUVD currently operates more as an aggregation layer than as a fully enriched and effective vulnerability database. The recommendations presented in this Policy brief address these limitations in a manner consistent with the API's existing design philosophy and the programmatic requirements of organisations operating under EU cybersecurity regulation. Given the EUVD's role within the NIS compliance ecosystem, prioritising these developer-oriented improvements would be expected to improve adoption and strengthen the database's position as a reliable, interoperable component of European cybersecurity infrastructure.

References

[1] https://www.greenbone.net
[2] https://euvd.enisa.europa.eu
[3] https://github.com
[4] https://www.osm-s.com
[5] https://www.enisa.europa.eu
[6] ENISA (2025). Consult the European Union Vulnerability Database to Enhance Your Digital Security. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security
[7] NIST to limit work on CVE entries as submissions surge | The Record from Recorded Future News https://therecord.media/nist-to-limit-work-on-cve-entries-surge?mkt_tok=Njc4LUZITC03MTAAAAGhM9mW1iYKjc_ClNWTFFMLUywhqHywIBYgmru8IdsM3d6nSS1hOdAUJiLixoZphRQFjbubCPtZ5r1MMyIDkNchK-DHB1WcPAfVivbWf6Rn
[8] VulnCheck (2025). Does ENISA EUVD Live Up to All the Hype? Technical Research Blog. https://www.vulncheck.com/blog/enisa-euvd
[9] Infosecurity Europe (2026). How to Use Europe's New Vulnerability Database. https://www.infosecurityeurope.com/en-gb/blog/future-thinking/how-to-use-euvd-enisa.html
[10] bytew0lf (2025). EUVD-API: EU Vulnerability Database API Documentation. GitHub Repository. https://github.com/bytew0lf/EUVD-API
[11] kaansk (2025). go-euvd: Comprehensive Go Library for the ENISA EUVD API. GitHub Repository. https://github.com/kaansk/go-euvd
[12] seifreed (2025). euvd-cli: European Union Vulnerability Database API Client. GitHub Repository. https://github.com/seifreed/euvd-cli
[13] European Parliament and Council of the EU (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union.
[14] European Parliament and Council of the EU (2024). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union.
[15] FIRST.org (2024). Exploit Prediction Scoring System (EPSS) Documentation. Forum of Incident Response and Security Teams. https://www.first.org/epss/

Appendix

Example API output - EUVD-2026-20884


```
{
    "id":"EUVD-2026-20884",
    "enisaUuid":"aaeb14a7-948f-3682-b96d-3d3653ecaa68",
    "description":"Hydrosystem Control System does not enforce authorization for some directories. This
allows an unauthorized attacker to read all files in these directories and even execute some of them.
Critically the attacker could run PHP scripts directly on the connected database.This issue was fixed in
Hydrosystem Control System version 9.8.5",
    "datePublished":"Apr 9, 2026, 12:31:10 PM",
    "dateUpdated":"Apr 9, 2026, 12:31:10 PM",
    "baseScore":8.8,
    "baseScoreVersion":"4.0",
    "baseScoreVector":"CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N",
    "references":"https://cert.pl/posts/2026/04/CVE-2026-
4901/\nhttps://www.hydrosystem.poznan.pl/\nhttps://nvd.nist.gov/vuln/detail/CVE-2026-34184\n",
    "aliases":"CVE-2026-34184\n",
    "assigner":"CERT-PL",
    "epss":0.0,
    "enisaIdProduct":[
        {
        "id":"f80e1300-f7e7-3826-97e3-fd13b19f5a73",
        "product":{"name":"Control System"},
        "product_version":"0 \u003c9.8.5"
        }
    ],
    "enisaIdVendor":[
        {
            "id":"1f17951f-6629-3406-a645-16649f25c312",
            "vendor":{"name":"Hydrosystem"}
        }
    ],
    "enisaIdVulnerability":[
        {
            "id":"9093c85e-17eb-38d1-a0f3-d6c934f6c959",
            "vulnerability":{
                "id":"GHSA-hh72-xj72-2c38",
                "datePublished":"Apr 9, 2026, 12:31:10 PM",
                "dateUpdated":"Apr 9, 2026, 12:31:10 PM",
                "baseScore":0.0,
                "references":"https://nvd.nist.gov/vuln/detail/CVE-2026-
34184\nhttps://cert.pl/posts/2026/04/CVE-2026-4901\nhttps://www.hydrosystem.poznan.pl\n",
                "enisa_id":"EUVD-2026-20884\nEUVD-2026-20885\n",
                "aliases":"CVE-2026-34184\n",
                "epss":0.0,
                "dataProcessed":"Apr 9, 2026, 4:00:18 PM",
                "vulnerabilityProduct":[],
                "vulnerabilityVendor":[]
            }
        },
        {
            "id":"be1c8a5c-1a19-3d72-a515-512e481b3623",
            "vulnerability":{
```

```
                "id":"CVE-2026-34184",
                "description":"Hydrosystem Control System does not enforce authorization for some directories. This allows an unauthorized attacker to read all files in these directories and even execute some of them. Critically the attacker could run PHP scripts directly on the connected database.This issue was fixed in Hydrosystem Control System version 9.8.5",
                "datePublished":"Apr 9, 2026, 9:41:08 AM",
                "dateUpdated":"Apr 9, 2026, 9:41:08 AM",
                "status":"PUBLISHED",
                "baseScore":8.8,
                "baseScoreVersion":"4.0",
                "baseScoreVector":"CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N",
                "references":"https://cert.pl/posts/2026/04/CVE-2026-4901/\nhttps://www.hydrosystem.poznan.pl/\n",
                "enisa_id":"EUVD-2026-20885\n",
                "assigner":"CERT-PL",
                "epss":0.0,
                "dataProcessed":"Apr 9, 2026, 2:00:32 PM",
                "vulnerabilityProduct":[{
                    "id":"0e1d2391-f3a7-3e56-84cd-ea6cd1da7ab4",
                    "product":{"name":"Control System"},
                    "product_version":"0 \u003c9.8.5"
                }],
                "vulnerabilityVendor":[{
                "id":"d832c529-23d3-31a5-b695-ecf1d3b7d825",
                "vendor":{"name":"Hydrosystem"}}]
            }
        }
    ],
    "enisaIdAdvisory":[]
}
```

TELEMETRY: Trustworthy mEthodologies, open knowLedgE & autoMated tools for sEcurity Testing of IoT software, haRdware & ecosYstems

TELEMETRY - 101119747

HORIZON-CL3-2022-CS-01-02

telemetry.eu info@telemetry.eu telemetry-project