SEAL

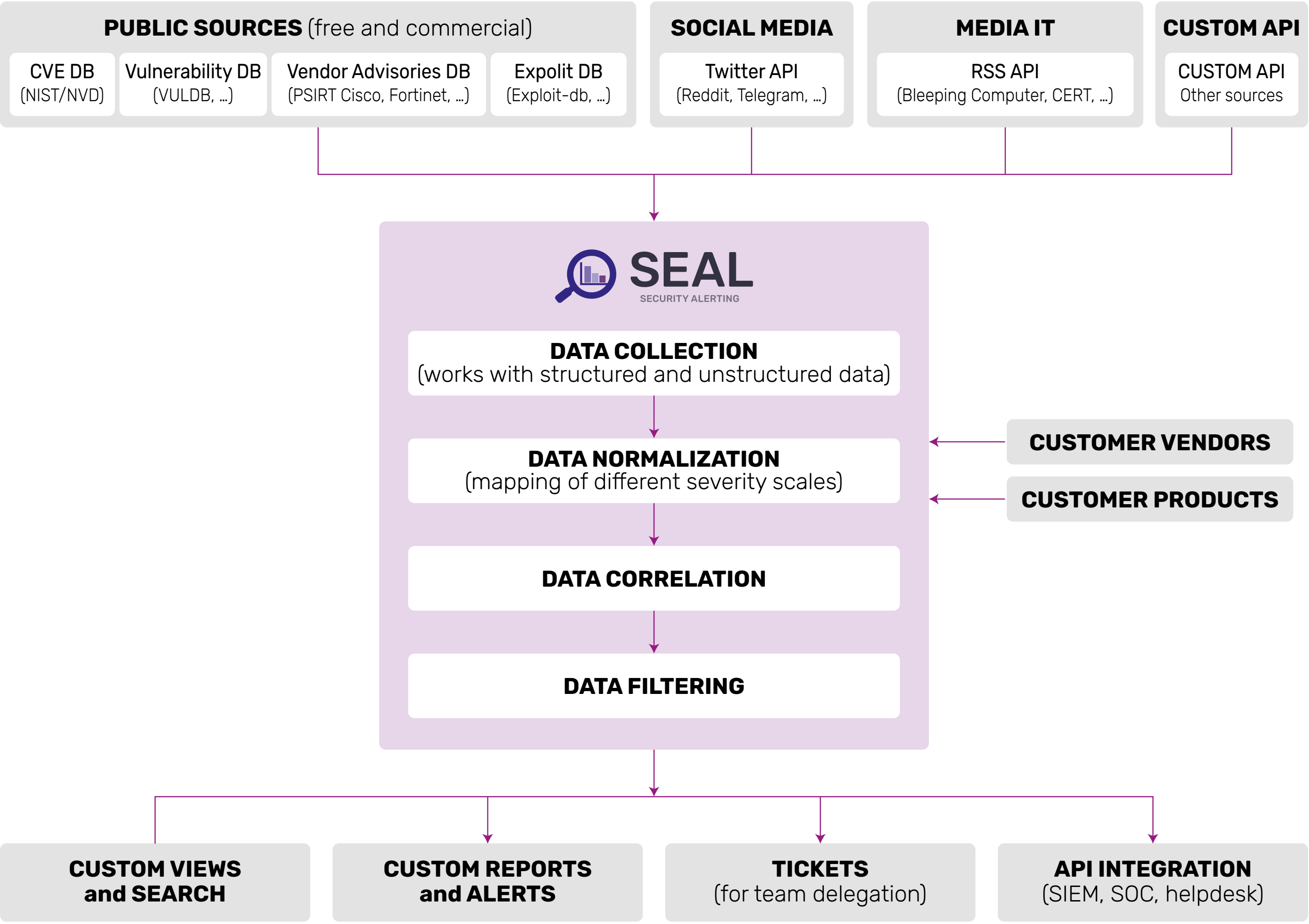
SECURITY ALERTING

THE SEAL SERVICE PROVIDES:

- □ SECURITY ALERTING
- □ VULNERABILITY INTELLIGENCE
- □ SECURE THE SOFTWARE SUPPLY CHAIN (SBOM)

SEAL integrates information about current vulnerabilities from a large number of different information sources. The focus is mainly on **zero-day vulnerabilities** which require a quick response. It further processes this information, **searches for connections in it** and filters it according to the configuration requirements of a specific customer. The advantage is that it allows the customer to connect any number of their **own sources**, including social networks.

„SEAL provides up-to-date information about the vulnerabilities of your systems and thus prevents their possible exploitation.“



PUBLIC SOURCES (free and commercial)

- CVE DB (NIST/NVD)
- Vulnerability DB (VULDB, …)
- Vendor Advisories DB (PSIRT Cisco, Fortinet, …)
- Expolit DB (Exploit-db, …)

SOCIAL MEDIA

- Twitter API (Reddit, Telegram, …)

MEDIA IT

- RSS API (Bleeping Computer, CERT, …)

CUSTOM API

- CUSTOM API Other sources

SEAL SECURITY ALERTING

- **DATA COLLECTION** (works with structured and unstructured data)
- **DATA NORMALIZATION** (mapping of different severity scales)
- **DATA CORRELATION**
- **DATA FILTERING**

CUSTOMER VENDORS

CUSTOMER PRODUCTS

- **CUSTOM VIEWS and SEARCH**
- **CUSTOM REPORTS and ALERTS**
- **TICKETS** (for team delegation)
- **API INTEGRATION** (SIEM, SOC, helpdesk)

KEY PRODUCT FEATURES

- □ **Comprehensive vulnerability information.**
- □ Tool for **security teams**.
- □ An easy-to-use portal for quick access to the latest vulnerabilities **(zero-day)**.
- □ Vulnerability detection from **various sources** – NIST, RSS, Twitter, CVE database, PSIRT, … or other customer-defined sources.
- □ Searching for the latest vulnerability in software – **third party libraries**.
- □ **Information about the source of the vulnerability**, extensive references such as links to patches or exploits.
- □ **Timeline of disclosure**, individual source types, and other vulnerability metadata.
- □ Search for **mutual connections** and a clear form of presentation to the user. Provides **mapping to CVE**.
- □ Definition of custom **„views“**, i.e. areas of interest, for easy filtering of only vulnerabilities of interest to the user or organization.

BASIC DESCRIPTION OF THE SEAL SERVICE

- □ The SEAL service is provided in the form of a cloud service (SaaS). The servers use the AWS platform.
- □ For special requirements, the SEAL service can be installed to the customer's on-premise environment.
- □ The SEAL service is a browser-based web application (no clients or agents).
- □ Customer user accounts are grouped into an organization / tenant.

COMPLIANT WITH NIS2 DIRECTIVE

Supply chain security

Vulnerability management

COMPLIANT WITH CISA RECOMMENDATIONS

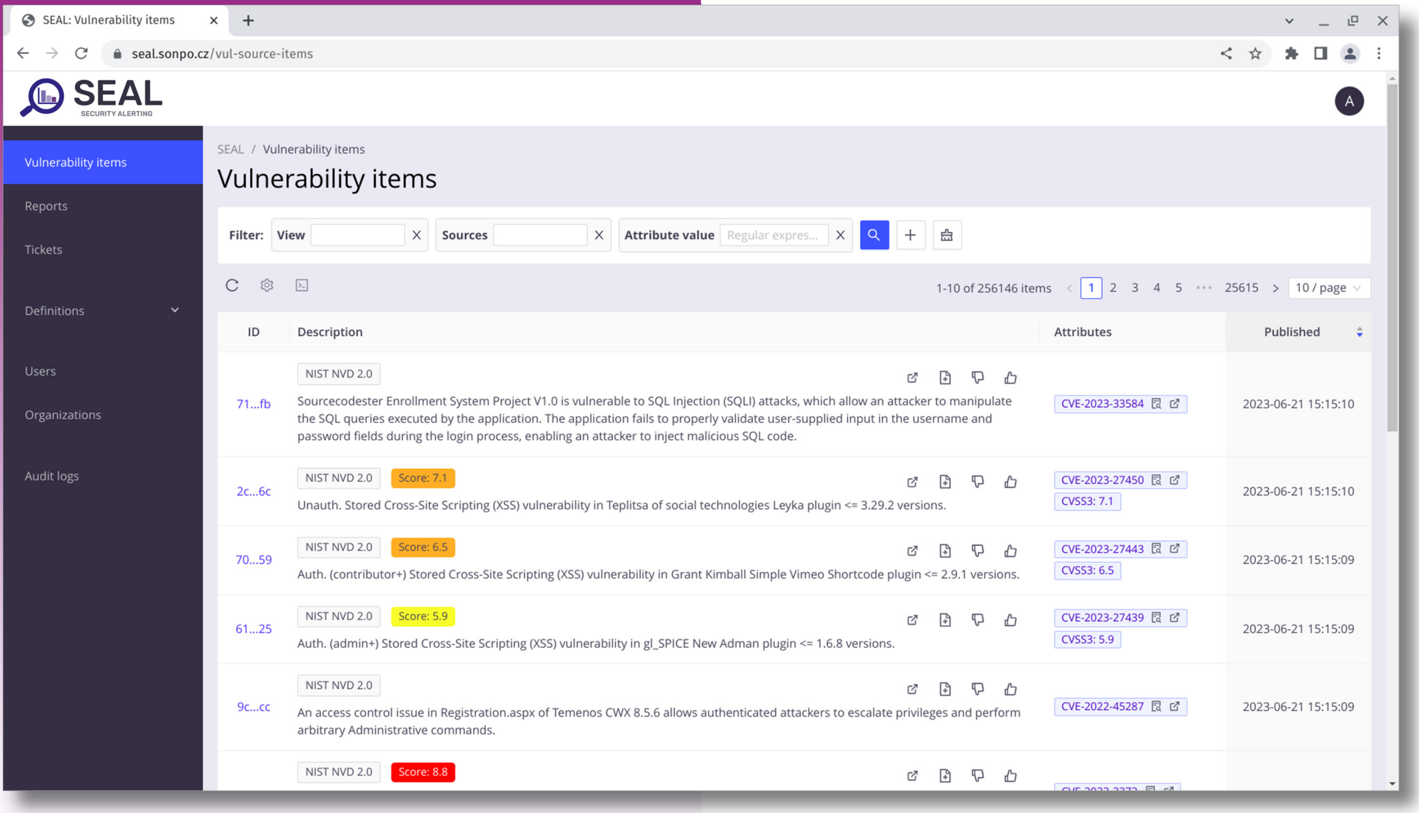
Secure the software supply chain (SBOM)

Vulnerability alerting and advisories

COMPLIANT WITH NUKIB RECOMMENDATIONS

Minimum safety standards

Recommendations for administrators



Vulnerability items

Filter: View | Sources | Attribute value: Regular expres...

1-10 of 256146 items < 1 2 3 4 5 ••• 25615 > 10 / page

ID	Description	Attributes	Published
71...fb	NIST NVD 2.0 Sourcecodester Enrollment System Project V1.0 is vulnerable to SQL Injection (SQLI) attacks, which allow an attacker to manipulate the SQL queries executed by the application. The application fails to properly validate user-supplied input in the username and password fields during the login process, enabling an attacker to inject malicious SQL code.	CVE-2023-33584	2023-06-21 15:15:10
2c...6c	NIST NVD 2.0 Score: 7.1 Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Teplitsa of social technologies Leyka plugin <= 3.29.2 versions.	CVE-2023-27450 CVSS3: 7.1	2023-06-21 15:15:10
70...59	NIST NVD 2.0 Score: 6.5 Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Grant Kimball Simple Vimeo Shortcode plugin <= 2.9.1 versions.	CVE-2023-27443 CVSS3: 6.5	2023-06-21 15:15:09
61...25	NIST NVD 2.0 Score: 5.9 Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in gl_SPICE New Adman plugin <= 1.6.8 versions.	CVE-2023-27439 CVSS3: 5.9	2023-06-21 15:15:09
9c...cc	NIST NVD 2.0 An access control issue in Registration.aspx of Temenos CWX 8.5.6 allows authenticated attackers to escalate privileges and perform arbitrary Administrative commands.	CVE-2022-45287	2023-06-21 15:15:09
	NIST NVD 2.0 Score: 8.8		

RISK RATINGS – OF VENDORS OR PRODUCTS

Comprehensive information about vulnerabilities of individual vendors or products. Find out which products and vendors put your organization at risk, including how quickly they respond to vulnerabilities and provide fixes.
Detailed historical data for a complete picture of a manufacturer or a product.

INFORMATION ABOUT THIRD PARTY LIBRARIES (SBOM)

A detailed overview of vulnerabilities in third-party libraries used in product and software development.
The SEAL application is the source of information for monitoring each library to ensure that newly discovered vulnerabilities are addressed through an update or other means. The information provides the customer with the ability to evaluate and select the best third-party libraries.

HISTORICAL DATA IN SEAL

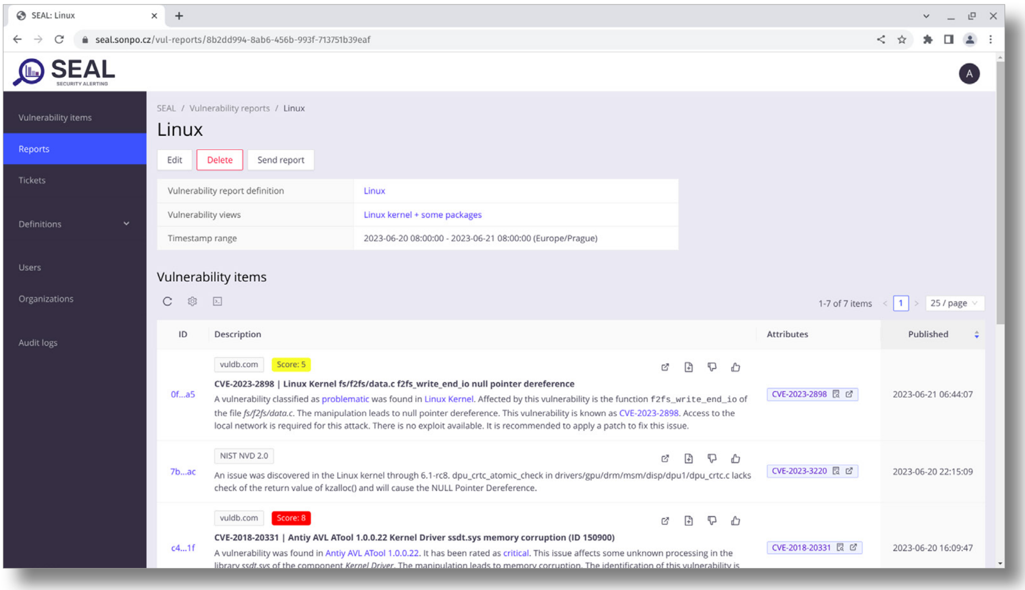
Historical data provide a complete picture of the evolution and connections of vulnerabilities. They help determine whether the product is safe and whether the manufacturer/vendor responds appropriately to security issues.

REPORTS AND ALERTS

Option to configure custom reports and alerts (E-mail, SMS, Signal, …) according to vendor, severity and other criteria. When a vulnerability is discovered or updated, information is sent to selected users or groups.

SERVICES OF OUR SPECIALISTS

Our dedicated team conducts further in-depth analysis of selected vulnerabilities to provide customers with comprehensive and most detailed information about the cause, impact and relationships of selected vulnerabilities.
We provide contractual SLA support 8×5 or 24x7 for our team of specialists.



Linux

Vulnerability report definition	Linux
Vulnerability views	Linux kernel + some packages
Timestamp range	2023-06-20 08:00:00 - 2023-06-21 08:00:00 (Europe/Prague)

Vulnerability items

1-7 of 7 items 1 25 / page

ID	Description	Attributes	Published
0f...a5	vuldb.com Score: 5 **CVE-2023-2898 | Linux Kernel fs/f2fs/data.c f2fs_write_end_io null pointer dereference** A vulnerability classified as problematic was found in Linux Kernel. Affected by this vulnerability is the function f2fs_write_end_io of the file *fs/f2fs/data.c*. The manipulation leads to null pointer dereference. This vulnerability is known as CVE-2023-2898. Access to the local network is required for this attack. There is no exploit available. It is recommended to apply a patch to fix this issue.	CVE-2023-2898	2023-06-21 06:44:07
7b...ac	NIST NVD 2.0 An issue was discovered in the Linux kernel through 6.1-rc8. dpu_crtc_atomic_check in drivers/gpu/drm/msm/disp/dpu1/dpu_crtc.c lacks check of the return value of kzalloc() and will cause the NULL Pointer Dereference.	CVE-2023-3220	2023-06-20 22:15:09
c4...1f	vuldb.com Score: 8 **CVE-2018-20331 | Antiy AVL ATool 1.0.0.22 Kernel Driver ssdt.sys memory corruption (ID 150900)** A vulnerability was found in Antiy AVL ATool 1.0.0.22. It has been rated as critical. This issue affects some unknown processing in the library *ssdt.sys* of the component *Kernel Driver*. The manipulation leads to memory corruption. The identification of this vulnerability is	CVE-2018-20331	2023-06-20 16:09:47

PSIRT ADVISORIES MANUFACTURERS

FORTINET
CHECK POINT
CISCO
paloalto NETWORKS
Microsoft

and others…

Cloud service SaaS

FREE TRIAL Request a FREE TRIAL

More information: **www.sonpo.cz**

SEAL is owned by:
SONPO, a.s. | Prague | Czech Republic
www.sonpo.eu | sales@sonpo.eu

Sonpo