



**Analysis of known
ICS vulnerabilities
for critical information
security decision-making**

The problem

Information on vulnerabilities found in ICS products and some common technological solutions for industrial enterprises is often riddled with serious errors and inaccuracies. This information is available in open sources and even provided by vendors. It frequently omits important details. Using such information carries the risk of missing an enterprise-critical vulnerability or wasting resources on neutralizing an essentially insignificant problem.

The solution

The use of reliable, up-to-date, analyzed data on known vulnerabilities in ICS products and other technological solutions used by enterprises, as well as detailed information on new vulnerabilities discovered by Kaspersky ICS CERT. Additionally, we provide recommendations on how to effectively mitigate vulnerabilities.

Kaspersky ICS Vulnerability Database was created by Kaspersky ICS CERT experts for cybersecurity professionals, threat analysts and risk managers who value accuracy and context.

- Unique data unavailable in public sources (NVD, CVE, etc.)
- A context verified by experts, not just lists of vulnerabilities
- Flexible delivery tailored to an organization's processes.

This data is essential for the effective prioritization of cybersecurity risks, the optimal protection of critical technological assets, and the justification of cybersecurity decisions.

Target audience

Industrial enterprises in various sectors, managed security service providers (MSSPs), security operations centers (SOCs), manufacturers of ICS products, cyber emergency response teams (CERTs), and information sharing and analysis centers (ISACs).

What's wrong with the data from public sources and vendors?

Inaccuracy

In our experience, vendors sometimes provide inaccurate information about vulnerable products. For example, they:

- do not provide an exhaustive list of product versions and configurations containing a vulnerable software component, which motivates customers to upgrade to new versions of their products, even if it is not necessary to fix a specific vulnerability;
- do not mention vulnerable products that are no longer supported;
- “forget” to mention an entire product line built on the same vulnerable codebase.

Such inaccuracies can lead to false-positive or false-negative results when assessing the security of systems on the industrial network by matching information on product versions used at an enterprise with the vendor's information on vulnerable products.

Obviously, the lack of vulnerability information for a particular version or configuration of the product is a serious problem. However, a too “general” description of the list of vulnerable versions and configurations has much more serious consequences than overlooking a single vulnerability. In such cases, it often results in “accept the risk and do nothing” decisions because the enterprise is simply incapable of updating a large number of systems.

In real-life, however, only some of the systems listed as vulnerable may actually require threat prevention measures (not necessarily updating), while some systems not on the list may also require such measures.

Difficulty of interpretation

Vulnerability data from public sources is often in a form that cannot be processed automatically. This makes automatically matching vulnerability data to the list of software or hardware versions used in the enterprise very difficult. Without a machine-readable format, the issue can only be resolved through time-consuming manual analysis by highly qualified personnel.

Controversial details of the vulnerability description

Vendors often provide minimal information in vulnerability descriptions: they fail to specify the conditions necessary to exploit a vulnerable product, do not identify the vulnerable component, and fail to provide an objective assessment of the possible consequences of using such a product.

These omissions lead to inaccurate assessments of the risks associated with attacks on vulnerable systems and suboptimal or incorrect decisions about risk mitigation and the necessary security measures.

Ineffectiveness of recommended mitigation measures

The mitigation measures recommended by a vendor may be redundant or, conversely, insufficient to protect against the alleged attack vector. Sometimes, the vendor suggests installing an update as the only protection measure, with no alternatives. Sometimes, the proposed update does not completely eliminate the vulnerability and leaves it susceptible to exploitation. Eliminating the vulnerability may not reduce the risk of an attack if there are architectural security problems in the system – patching a hole in the fence makes no sense when the gate is wide open.

What we offer

Kaspersky ICS Vulnerability Database

The database contains verified, corrected and up-to-date information on known vulnerabilities in ICS products and other solutions widely used in enterprises' technological environments, as well as new vulnerabilities discovered by Kaspersky ICS CERT. When installing an update is impossible or insufficient to mitigate the risk, we suggest alternative ways to eliminate or complicate exploitation of each vulnerability.

Kaspersky ICS Vulnerability Database includes:

- Corrected and supplemented information on the vulnerability, its severity level, and the mechanisms and possible consequences of its exploitation.
- A detailed list of products that includes only those models/versions/equipment/configurations of the product that actually contain the vulnerability.
- A full name for each model/version of the product according to the vendor's notation, with information on specific firmware versions for devices, as well as machine-readable designation.

- An extended list of vulnerability mitigation measures with comments on the vendor's recommendations, and alternative approaches.

Complete and reliable vulnerability information helps ensure that informed decisions are made when developing a mitigation plan and a set of mitigation measures, reducing associated costs as well as cybersecurity risks in general.

What we do

Researching new and analyzing known vulnerabilities

We identify and research new vulnerabilities in popular ICS products and analyze known flaws. All the results are entered into the database as they become available.

Constantly monitoring the main sources of information

We monitor all major sources of vulnerability information, including MITRE, NVD, US-CERT, major software and equipment vendors, and publications by security researchers who discovered the vulnerability.

Thoroughly analyzing data

Vulnerability data included in the Kaspersky ICS Vulnerability Database is meticulously verified and analyzed for completeness and reliability.

Updating the list of vulnerable products

We research vendors' product lines and examine their functionality and component base to check and update the list of vulnerable products. We record all models/versions/equipment/configurations exposed to vulnerabilities.

Searching for information on vulnerabilities in third-party technologies used in industrial control systems

Special emphasis is placed on vulnerabilities in third-party technologies that are widely used in ICS solutions and on finding information about end products that use common components.

Providing relevant recommendations on ways to fix vulnerabilities

A list of recommendations is compiled for each vulnerability, detailing how it can be closed based on our own expertise and on best practices.

What the customer gets

Essential information about vulnerabilities

- CVE;
- vulnerability description;
- exploitation conditions and consequences;
- CVSS score and vector;
- list of products affected by the vulnerability in which each record is a machine-readable product name with a specific version according to the CPE (Common Platform Enumeration) standard;
- extended list of recommendations for fixing the vulnerability, including alternative methods and an expert assessment of the effectiveness of installing vendor-provided updates.

The data is provided both in the form of regular, human-readable reports, and in the form of a JSON data stream.

[Request a consultation](#)

Related services

- ICS vulnerability data feed
- Product vulnerability assessment
- IoT vulnerability research. Training
- Analytical reports on ICS threats and vulnerabilities on the Kaspersky Threat Intelligence Portal

[Request a consultation](#)

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT)

is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

[Kaspersky ICS CERT](#)

ics-cert@kaspersky.com