KASPERSKY lab

INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES STATISTICS

Oxana Andreeva, Sergey Gordeychik, Gleb Gritsai, Olga Kochetova, Evgeniya Potseluevskaya, Sergey I. Sidorov, Alexander A. Timorin

Table of Contents

1 Introduction

1.1 Overview

Industrial control systems (ICS) surround us: they are used across multiple sectors including electricity, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). Smart cities, smart houses, smart cars, and medical equipment – all of these are driven by ICS.

The number of ICS components available over the Internet increases every year, and the expansion of the Internet makes ICS easy prey for attackers. Taking into account that, initially, many ICS solutions and protocols were designed for isolated environments, their new online availability can make it possible for a malicious user to cause impact on the infrastructure behind the ICS, due to its lack of Internet-ready security controls. Moreover, some components are vulnerable themselves. The first information about vulnerabilities in ICS components became available in 1997, when only two vulnerabilities were published. Since then the number of vulnerabilities has significantly increased. Over the past five years, this index has increased from 19 vulnerabilities in 2010 to 189 vulnerabilities in 2015.

Sophisticated attacks on ICS systems are not new anymore. Here, it is worth remembering the 2015 incident in Ivano-Frankivsk, Ukraine, where around a half of the area's houses were left without electricity because of a cyber-attack against the Prykarpattyaoblenergo power company. It was only one of multiple victims of the BlackEnergy1 APT campaign.

Another notable incident in 2015, described in the Verizon Data Breach Digest2, was an attack on the Kemuri Water Company's ICS infrastructure. Intruders infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water. The intrusion was performed through a vulnerable externally available system, which managed the programmable logic controllers (PLCs) regulating the valves and ducts that controlled the flow of water and chemicals used through the system.

In 2015, there were other reports of ICS-related incidents, such as attacks on a steel mill in Germany and on the Frederic Chopin Airport in Warsaw[3].

This report provides an overview of the current worldwide situation with ICS security, looking at vulnerabilities, and the vulnerable ICS components exposed to the Internet.

1.2 Analysis Approach

The research is focused on two areas: Vulnerabilities and ICS Availability over the Internet. This report is dedicated to the first part of the research results – ICS Vulnerabilities in 2015. Information gathering on vulnerabilities was carried out using open sources, such as Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) advisories, NVD/CVE, SCADA Strangelove, Siemens Product CERT and other information available online. Severity levels for the vulnerabilities were assessed based on the Common Vulnerability Scoring System (CVSS) versions 2 and 3. CVSS v2 was used to compare vulnerability statistics in the years 2014 and 2015, and it was also used for any vulnerabilities that didn't have a CVSS v3 score assigned.

---

[1] https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

[2] http://www.verizonenterprise.com/verizon-insights/data-breach-digest/2016/

[3] https://securelist.com/analysis/kaspersky-security-bulletin/72886/kaspersky-security-bulletin-2015-top-security-stories/

2 Main Findings

The main findings of the research are as follows:

- **The number of vulnerabilities in ICS components keeps growing**. With increased attention to ICS security over the last few years, more and more information about vulnerabilities in these systems is becoming public. However, the vulnerabilities themselves could be present in these products for years before they are revealed. In total, 189 vulnerabilities in ICS components were published in 2015, and most of them are critical (49%) or have medium severity (42%).
- **Vulnerabilities are exploitable**. For 26 of the vulnerabilities published in 2015, exploits are available. Besides, for many vulnerabilities (such as hard-coded credentials) an exploit code is not needed at all to obtain unauthorized access to the vulnerable system. Moreover, our ICS security assessment projects show that ICS are often considered by their owners as “black boxes”, so default credentials in ICS components are often not changed and could be used to gain remote control over the system.
- **ICS vulnerabilities are widely diversified**. New vulnerabilities were found in 2015 in the ICS components of different vendors (55 different manufacturers) and types (HMI, electric devices, SCADA, industrial network devices, PLCs and multiple others). The largest amount of vulnerabilities were found in Siemens, Schneider Electric and Hospira devices. Vulnerabilities in ICS components have a different nature. The most widespread types are buffer overflows (9% of all detected vulnerabilities), use of hard-coded credentials (7%), and cross-site scripting (7%).
- **Not all of the vulnerabilities found in 2015 are fixed**. Patches and new firmware are available for 85% of the published vulnerabilities, the rest are not fixed or are only partially fixed for different reasons. Most of the unpatched vulnerabilities (14 out of 19) are of high level risk. These unpatched vulnerabilities pose significant risk to the owners of the corresponding systems, especially to those who, due to inappropriate network configuration management, have their vulnerable ICS systems exposed to the Internet. Examples include the 11,904 remotely available SMA Solar Sunny WebBox interfaces that are under risk of compromise though hard-coded passwords. Although for Sunny WebBox this number has significantly reduced since 2014 (when over 80 thousand available componenets were found[4]), the amount is still high, and the unfixed hard-coded credentials issue (published in 2015) is now putting these systems at much higher risk than was previously thought.

[4] http://scadastrangelove.blogspot.ru/2016/02/scadasos-annual-report.html

3 Vulnerabilities

3.1 Overview

The first publically available information on vulnerabilities in ICS components dates back to 1997, when two vulnerabilities were published. Since then, the number of annually revealed vulnerabilities has significantly increased. Over the past five years, this index has increased from 19 vulnerabilities in 2010 to 189 vulnerabilities in 2015. In 2010-2012 there was a period of sharp growth in the number of vulnerabilities, reflecting the increased attention that researchers and system owners paid to the problem of ICS IT security during this time. These efforts have now been superseded by a period of active research: every year over 150 vulnerabilities are detected, and the average number of ICS vulnerabilities almost matches this.

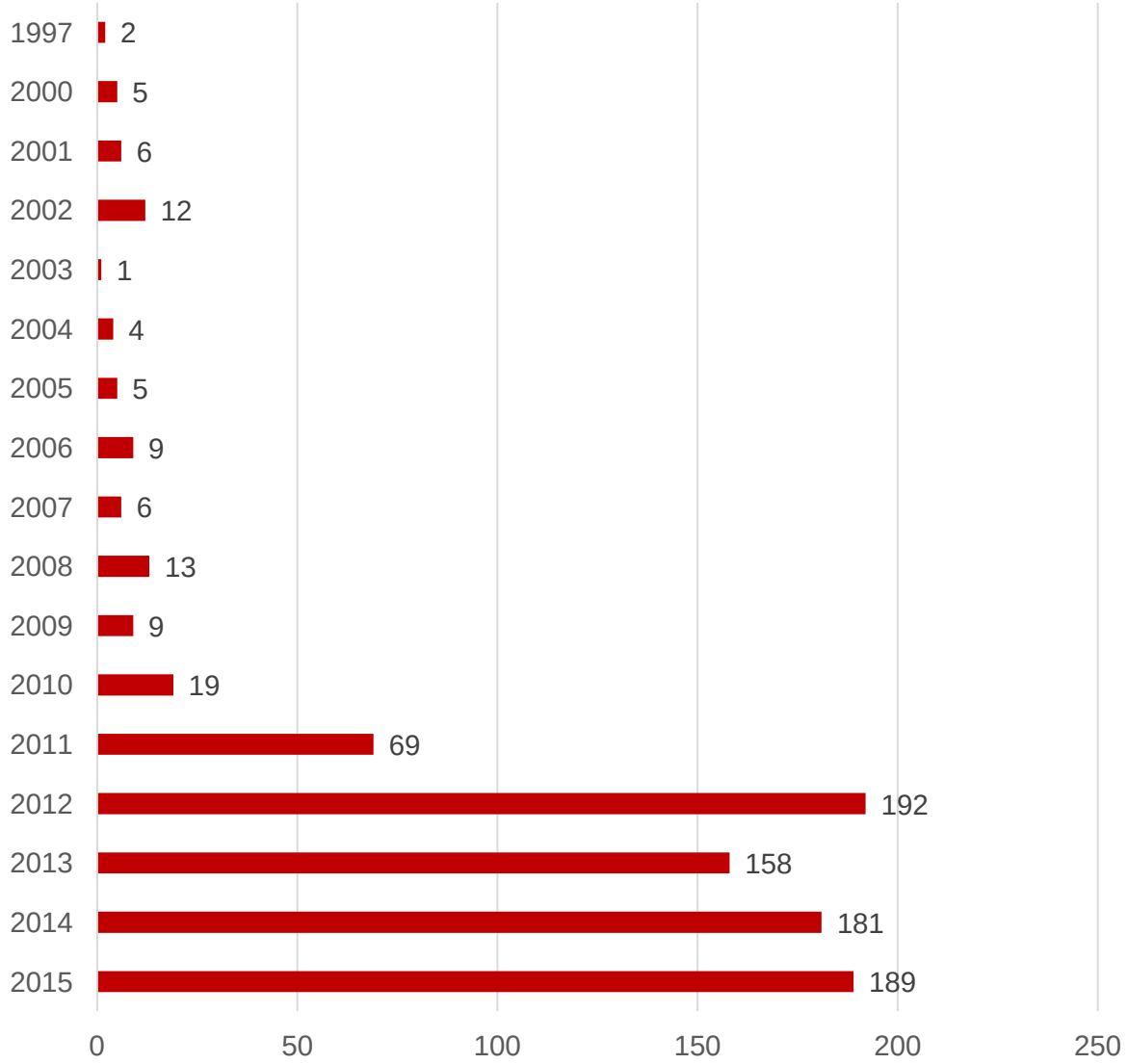

Figure 1. ICS vulnerabilities by year

In 2015, most of the detected vulnerabilities were of medium (54%) or high (34%) risk levels, according to CVSS v2 base scores.

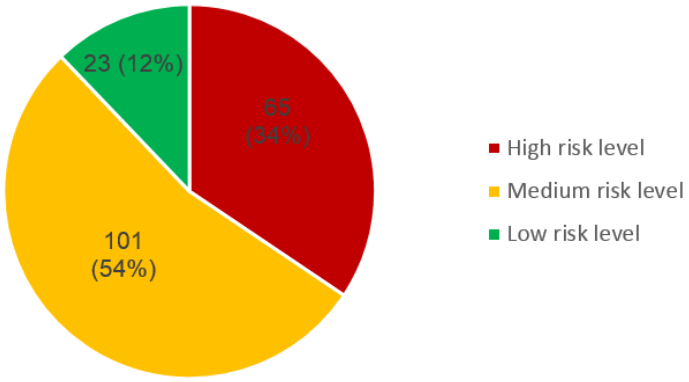

Figure 2. ICS vulnerabilities in 2015 by risk level (CVSS v2)

Compared to 2014, the share of critical vulnerabilities has decreased by 15%, and the percentage of medium level vulnerabilities has increased by 9%.

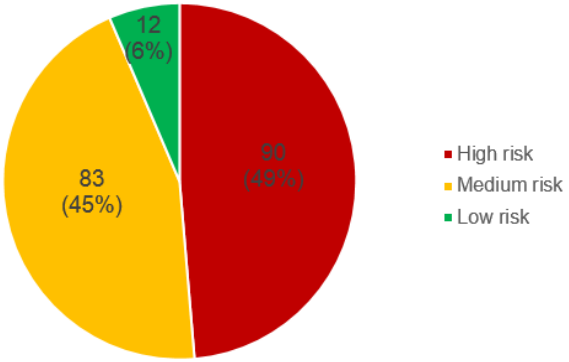

Figure 3. ICS vulnerabilities in 2014 by risk level (CVSS v2)

However, in 2015 a new vulnerability severity scoring system was introduced – CVSS v3. It is based on more parameters, and, thus, more accurately evaluates severity levels. We have considered the CVSS v3 base scores for vulnerabilities, and ICS-CERT, and CVSS v2 base scores for the rest of the security flaws. The resulting statistics were less optimistic compared to those based purely on CVSS v2: here 49% of vulnerabilities are critical, and 42% are of medium risk.

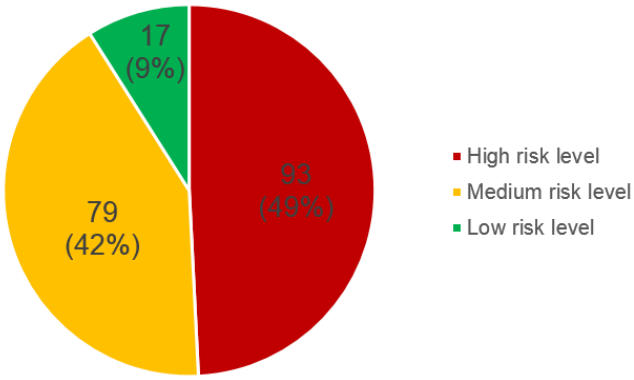

Figure 4. ICS vulnerabilities in 2015 by risk level (CVSS v2 and CVSS v3)

For 26 of the vulnerabilities published in 2015, exploits are available (these vulnerabilities are currently fixed). Here are examples of the vulnerabilities with exploits:

- **NTP Symmetric Association Authentication Bypass Vulnerability (CVE-2015-7871)** of medium risk. An attacker could potentially make the NTP daemon accept time updates from non-specified NTP servers by sending specially crafted UDP packets to the NTP service, which may lead to an **authentication bypass** in Siemens Ruggcom Rox II (if the NTP service is activated).
- **Glibc Ghost Vulnerability (CVE-2015-0235)**. SINUMERIK 808D, 828D, 840D sl, all versions up to 4.7, and SIMATIC HMI Basic Panels 2nd Generation are subjected to the "GHOST" vulnerability. Incorrect parsing within the glibc library functions "gethostbyname()" and "gethostbyname2()" allows a context-dependent attacker to **execute arbitrary code**.
- **Multiple Mango Automation 2.6.0 Vulnerabilities**. An attacker could **execute arbitrary HTML and script code** in a user's browser session (CVE-2015-6494), **obtain sensitive information** (CVE-2015-7900), **enumerate valid users** on the affected node (CVE-2015-7902), **execute arbitrary JSP code** by uploading a malicious JSP script file (CVE-2015-7904), **execute arbitrary SQL commands** (CVE-2015-7903), **inject and execute arbitrary OS commands** as well as use cross-site request forgery attacks (CVE-2015-7901) and **hijack the authentication** (CVE-2015-6493).
- **Schneider Electric Modicon PLC Vulnerabilities**. Ethernet communication modules: BMXNOC0401, BMXNOE0100, BMXNOE0110, BMXNOE0110H, BMXNOR0200H, BMXP342020, BMXP342020H, BMXP342030, BMXP3420302, BMXP3420302H and BMXP342030H are prone to **Reflected Cross-Site Scripting** (CVE-2015-6462) and **Remote File Inclusion** (CVE-2015-6461) vulnerabilities. An attacker could craft a specific URL, which contains Java script that will be executed on the client browser, or craft a specific URL referencing the PLC web server, which, when launched, will result in the browser redirecting to a remote file via a Java script loaded with the web page.
- **Authentication Bypass Vulnerability (CVE-2015-7938)**. An attacker is able to bypass authentication to access the Advantech EKI-132x platform devices.
- **Multiple Janitza UMG Power Quality Measuring Products Vulnerabilities**. Power analyzers: UMG 508, UMG 509, UMG 511, UMG 604, and UMG 605 are affected by seven vulnerabilities. A remote attacker could **obtain access** via a brute-force attack (CVE-2015-3972), **determine a PIN value** via unspecified computations on session-token values (CVE-2015-3973), **read or write to files** via a session on TCP port 21 (CVE-2015-3968), **read or write to files, or execute arbitrary JASIC code**, via a session on TCP port 1239 (CVE-2015-3971), **inject arbitrary web script or HTML** (CVE-2015-3970), **hijack the authentication of arbitrary users** (CVE-2015-3967) and **obtain sensitive network-connection information** via a request to the UDP port 1234 or 1235 (CVE-2015-3969).
- **AMX Multiple Products Credential Management Vulnerability**. Harman AMX devices before 2015-10-12 are prone to the CVE-2015-8362 vulnerability. Affected devices contain a **hard-coded password** for a diagnostic account with elevated privileges that can be used to configure user settings, device settings, upload files, and download files.
- **Yokogawa CENTUM CS 3000 Buffer Overflow Vulnerability**. The CVE-2015-5626, CVE-2015-5627 and CVE-2015-5628 vulnerabilities in Yokogawa CENTUM CS 3000 allow a remote attacker to overwrite the buffer.

- **Elipse E3 DLL Hijacking Vulnerability**. Using the CVE-2015-0978 vulnerability an attacker might be able to gain privileges in Elipse E3 4.5.232 through 4.6.161 via a Trojan horse DLL in an unspecified directory.
- **SearchBlox v8.3 Information Exposure Vulnerability**. The config file can be overwritten without admin login. This could allow the attacker to cause a crash (CVE-2015-7919).
- **Moxa VPort ActiveX SDK Plus Buffer Overflow Vulnerability**. A function in ActiveX has the CVE-2015-0986 vulnerability. Successful exploitation of this vulnerability may allow the insertion of lines of assembly code such as a call to another tool.

The existence of ready exploits simplifies a possible attack. As to other vulnerabilities, the absence of public exploits does not mean that risks posed by them should be ignored. Exploits could be developed by attackers individually for a target system, a common practice for highly-skilled malefactors, who are usually behind modern APT campaigns targeting critical infrastructures.

Besides, vulnerabilities related to hard-coded credentials usually do not require a special exploit to obtain unauthorized access to the vulnerable system, as knowledge of the hardcoded account, and an ability to perform an authentication attempt could be enough to log in to the system under the compromised account. Moreover, multiple web application vulnerabilities could be revealed and exploited by an attacker using regular web browsers and widespread application analysis tools.

3.2 Bug Fixes

In this section we provide statistics on vulnerability remediation based on official ICS-CERT data. However, the below statistics represent only a part of the security flaws that actually still exist in ICS components. There are many other vulnerabilities already known to vendors, but they were provided to the vendors via private research following a responsible disclosure policy. Such vulnerabilities are not published at the moment because the corresponding patches are not yet released. Besides, some security flaws are not officially acknowledged by vendors as vulnerabilities, however these peculiarities could still be used by attackers. For instance, a hard-coded confirmation code to access extended internal statistics and test information on a Siemens SIPROTEC 4 and SIPROTEC Compact[5].

If we consider data from ICS-CERT, vendors have produced **patches and new firmware for 85%** of the published vulnerabilities. At the same time **5% of vulnerabilities were not fully fixed**: released patches were only for certain versions of firmware and products, but not for all affected systems. For example, there are three high-risk vulnerabilities in the Yokogawa CENTUM series. The vendor has released a revision for CENTUM VP, however CENTUM CS 1000 and CENTUM CS 3000 are still vulnerable. For these products Yokogawa has provided recommendations to minimize risks associated with the vulnerabilities. **6% of vulnerabilities were not patched** because the vulnerable component was removed from the market or because a vendor does not support the product anymore (Figure 5).

[5] http://scadastrangelove.blogspot.com/2015/12/now-declared-capabilities.html

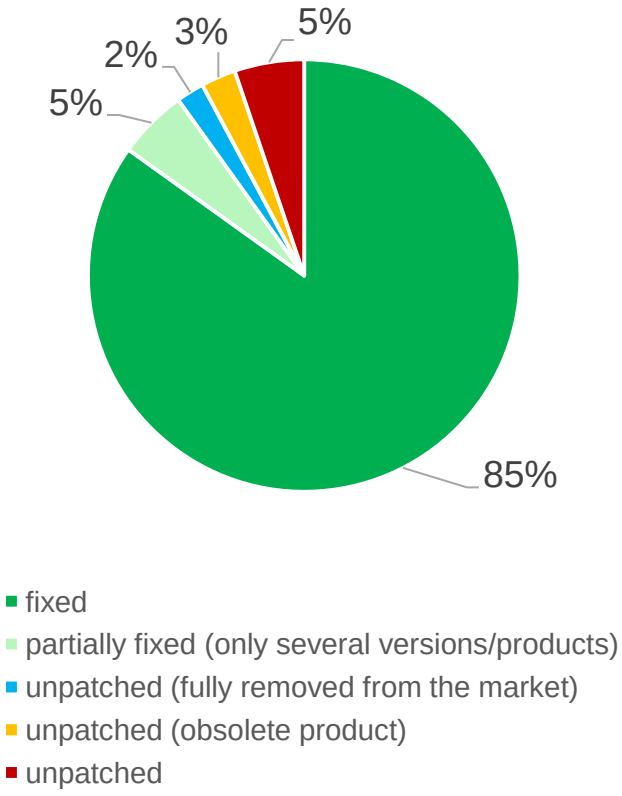

Figure 5. ICS patching

In total, by the end of 2015, **19 vulnerabilities remained unpatched**, including five medium risk vulnerabilities and 14 vulnerabilities of high risk (Figure 6).

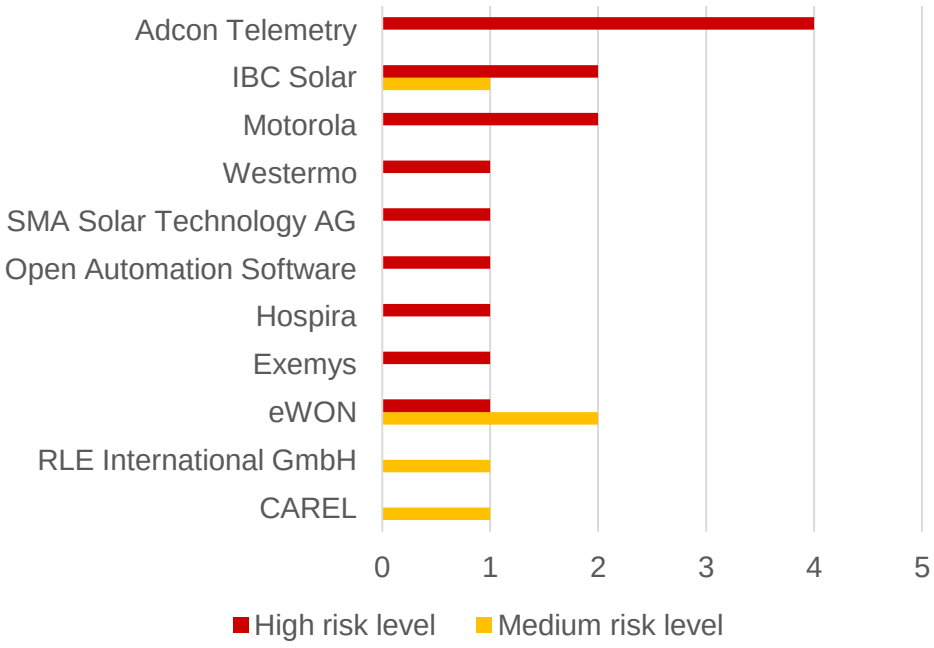

Figure 6. Unpatched vulnerabilities by vendor

The most widespread types of unfixed vulnerabilities are the **use of hard-coded credentials** (three vulnerabilities) and **cross-site request forgery** (two vulnerabilities). The unfixed vulnerabilities are as follows:

- **Adcon Telemetry Gateway A840 Base Station is prone to hard-coded credentials (CVE-2015-7930), improper authentication (CVE-2015-7931), the cleartext transmission of sensitive information (CVE-2015-7932) and information exposure (CVE-2015-7934) vulnerabilities.** An attacker could log into the device using the hard-coded credentials that grant administrative access.

  The system does not support SSL for encrypting network level communication. Because the support is not available in the Java client, the network communication is plaintext, and all data is transmitted in plaintext (improper authentication).

  Because there is no SSL support, the communication is not encrypted, making it easily readable over the network (cleartext transmission of sensitive information).

  The Java client is also used in the A840 gateway systems, revealing the full path of log files on the server (information exposure).

  Adcon Telemetry has stated that the A840 is an obsolete product and is no longer supported. No patches or updates will be created for this product.
- **IBC Solar ServeMaster TLP+ and Danfoss TLX Pro+ are affected by cross-site scripting (CVE-2015-6475) and source code disclosure (CVE-2015-6469) vulnerabilities.** Multiple cross-site scripting vulnerabilities allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. Also because of incorrect settings of the interpreter, the attacker can get the source code of executable scripts. IBC Solar has not produced a patch to mitigate this vulnerability.
- **All versions of Motorola MOSCAD IP Gateway are affected by Remote File Inclusion (CVE-2015-7935) and Cross-Site Request Forgery (CVE-2015-7936) vulnerabilities.** Files can be accessed and downloaded without authentication. Cross-Site Request Forgery attacks allow remote intruders to hijack the authentication of administrators for password change requests. Motorola Solutions has confirmed this product was cancelled at the end of 2012 and it no longer offers software updates.
- **The hard-coded credentials vulnerability (CVE-2015-7923) is present in Westermo WeOS before 4.19.0.** The SSL keys used by the switches to provide secure communications are hard-coded. Malicious parties could obtain the key, stage a man-in-the-middle attack by posing to be a WeOS device, and then obtain credentials entered by the end-user. With those credentials, the malicious party would have authenticated access to that device. Westermo is working on an update to automate the changing of the key, and this will be published on its website as soon as it is ready.
- **SMA Solar Sunny WebBox can be accessed using hard-coded passwords** that cannot be changed or disabled by a user (**CVE-2015-3964**). SMA is planning to discontinue the sale of this product, and there is no plan to fix old versions.
- **Uncontrolled search path element vulnerability (CVE-2015-7917) exists in Open Automation Software OPC Systems.NET Version 8.00.0023 and previous versions.** A successful exploit of this vulnerability requires the local user to install a crafted DLL on the victim machine. The application loads the DLL and gives the attacker access at the same privilege level as the application. Open Automation Software has reviewed the vulnerability and decided not to patch the issue at this time.
- **Hospira Symbiq Infusion System, Version 3.13 and prior versions are prone to exposed dangerous method or function (CVE-2015-3965).** With remote access

and elevated privileges, the Symbiq Infusion System can be remotely directed to perform unanticipated operations. As previously announced by Hospira in 2013, the Symbiq Infusion System was retired on May 31, 2015, and was fully removed from the market by December 2015.

- **Authentication bypass vulnerability (CVE-2015-7910) in Exemys Telemetry Web Server** allows an attacker to directly access information by ignoring the location header. Exemys has not produced a patch to mitigate this vulnerability.
- **Cross-Site Request Forgery (CVE-2015-7925) in eWON firmware versions prior to 10.1s0** is an exploit that allows for potential malicious commands to be passed from a user to the application server. The eWON web application contains a global Cross-Site Request Forgery vulnerability. There is no anti-CSRF token in use, either per page or per (configuration) function. An attacker can perform actions with the same permissions as the victim user, provided the victim has an active session and is induced to trigger the malicious request. Successful exploitation may allow execution of firmware upload, device reboot, or deletion of device configuration. eWON recommends using the router in a secure environment.

Unpatched vulnerabilities pose significant risks to the owners of corresponding systems, especially to those who, due to inappropriate network configuration management, have their vulnerable ICS systems exposed to the Internet, such as:

- **11,904 remotely available SMA Solar Sunny WebBox** interfaces are at risk of compromise though hard-coded passwords, which could be used to cause denial of service of the PV plant monitoring system. Among identified owners of the vulnerable devices there are electrical companies, a chemical company, and grocery stores.
- **57 hosts with remote availability through the Telnet protocol Adcon Telemetry Gateway A840**, which could be compromised by using a hard-coded password for a privileged user. Among identified owners there is agricultural equipment, as well as wine and fruit manufacturers.
- **One host with a remotely available Motorola Moscad IP Gateway**, where obtaining control over the device is possible for remote attackers through the Remote File Inclusion and Cross-Site Request Forgery attacks.

More information on ICS systems available through external networks is available in the second part of this research.

3.3 Vulnerabilities by Vendors

The largest amount of critical vulnerabilities in 2015 was identified in the products of vendors such as **Siemens (five critical vulnerabilities) and Schneider Electric (five critical vulnerabilities)**. Siemens, Schneider Electric and Hospira products have the highest total number of vulnerabilities found in their products: with 33, 18 and 12 vulnerabilities correspondingly.

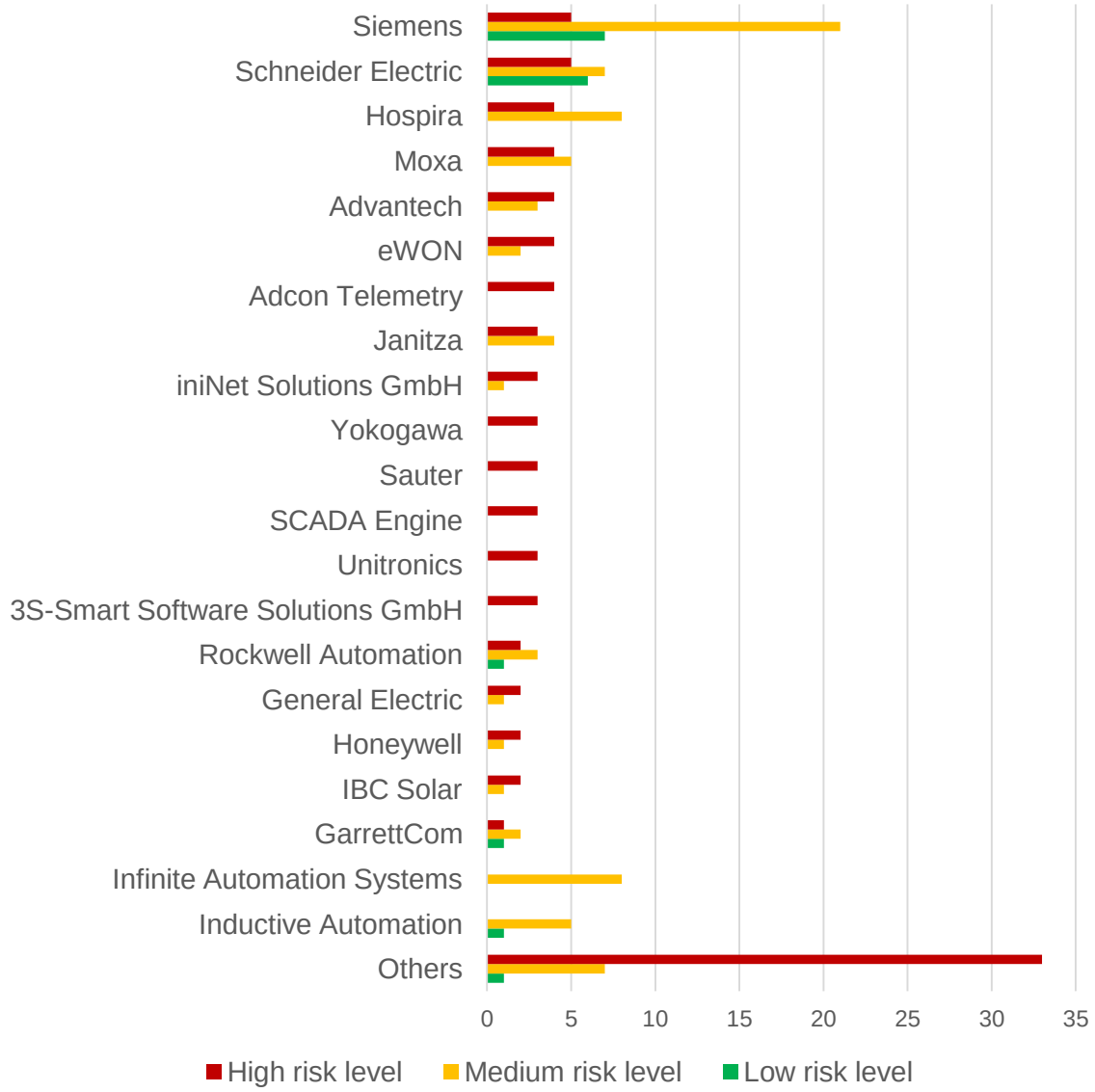

Figure 7. ICS vulnerabilities by vendor

Below are some examples in products of different vendors.

Siemens SICAM MIC devices with firmware before 2404 are exposed to the CVE-2015-5386 vulnerability that has a high risk level. Using this vulnerability, a remote attacker could bypass authentication and obtain administrative access to the device via unspecified HTTP requests.

Honeywell XLWeb controllers have a high risk vulnerability (CVE-2015-0984) allowing remote attackers to read files under the web root, and consequently obtain administrative login access via a crafted pathname. The XLWEB application effectively becomes an entry point into the network where it is located.

Multiple **Yokogawa** products have three critical vulnerabilities. All of them are related to stack-based buffer overflow attacks, which could lead to unresponsive network communications (CVE-2015-5626), executing arbitrary code (CVE-2015-5627) or making the communication function unavailable (CVE-2015-5628).

The high risk vulnerability CVE-2015-3977 is present in **Schneider Electric IMT25 Magnetic Flow DTM** before 1.500.004. A specific memory value can be overwritten by

sending a special reply to a HART command. The overwritten memory value can cause a denial of service and remote code execution.

Honeywell Midas gas detectors before 1.13b3 and **Midas Black gas detectors** before 2.13b3 are exposed to the CVE-2015-7907 vulnerability that has a high risk level. Using this vulnerability a remote attacker could bypass authentication, write to a configuration file or trigger a calibration or test, via unspecified vectors.

However, the list of vulnerable products is longer. 34 vendors are unified under the "others" category: Beckhoff, Emerson, Motorola, Mitsubishi Electric, etc. Each of these systems has one or two vulnerabilities.

3.4 Vulnerabilities by ICS Component Types

In 2015, the most vulnerable ICS components were HMI, Electric Devices and SCADA systems. The “Electric Device” category consists of distance protection devices, gas detectors, pumps, power analyzers, recloser control and relay platform units. The graph ниже demonstrates the vulnerability severity distribution for different types of ICS components.

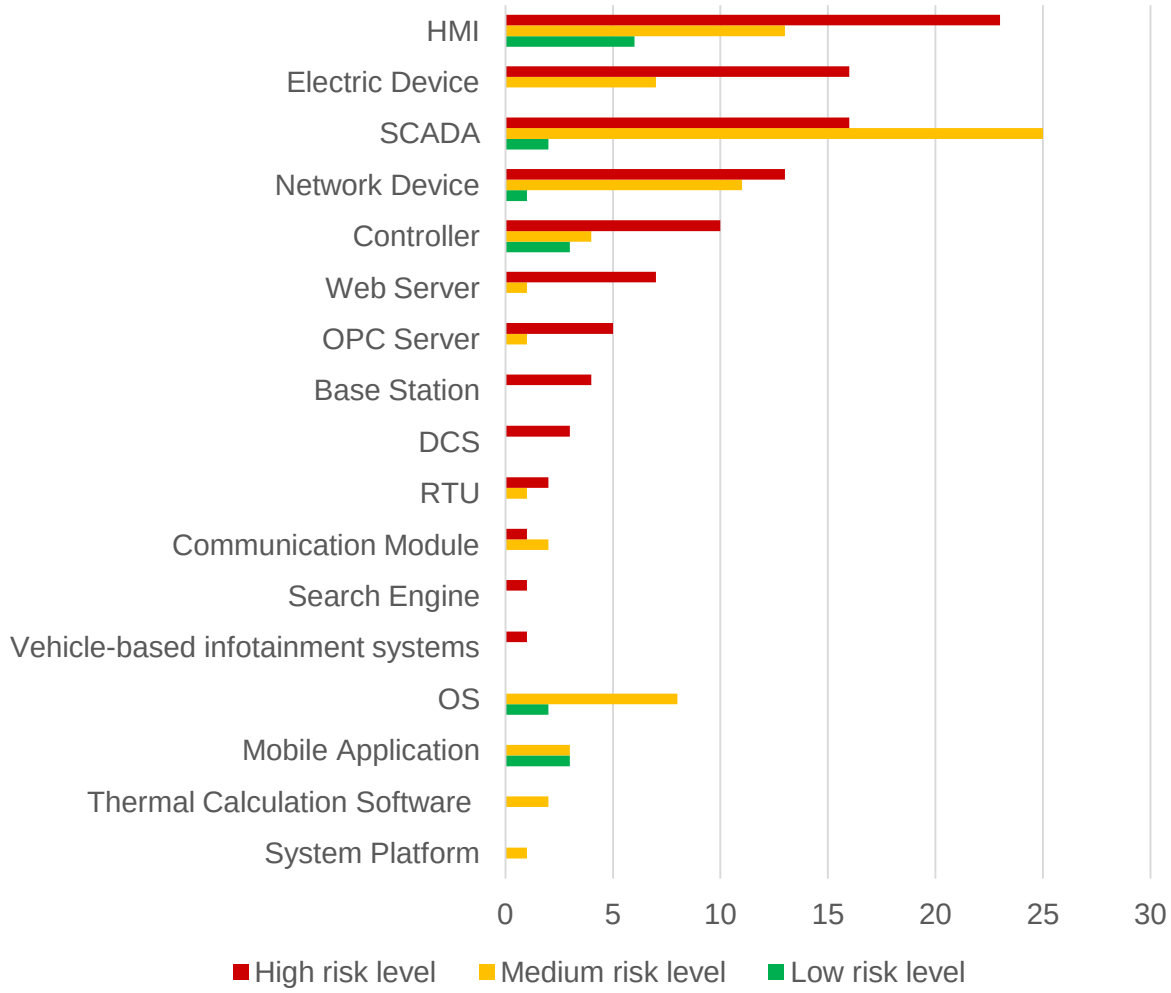

Figure 8. The number of vulnerabilities in different types of the ICS components by risk level

Among **HMI vulnerabilities** the most widespread types are **buffer overflows** (eight vulnerabilities), **cleartext transmission of sensitive information** (three vulnerabilities), use of **hard-coded credentials** (three vulnerabilities) and **storing passwords in a recoverable**

format (three vulnerabilities). One of examples is an Improper Access Control vulnerability (CVE-2015-4051, high risk level) in Beckhoff IPC Diagnostics before 1.8 (HMI) allowing an unauthenticated attacker to perform a variety of actions on the system by sending a specially crafted packet. These actions include rebooting the device or injecting a new user that has admin access rights on both the underlying embedded Windows and a web server.

For **electric devices** the most widespread issue is use of **hard-coded credentials** (three vulnerabilities). For instance, seven vulnerabilities exist in Hospira Plum A+ and Symbiq Infusion Systems products, intravenous pumps that deliver medication to patients: Key Management Errors (CVE-2015-3957), Cleartext Storage of Sensitive Information (CVE-2015-3952), Stack-Based Buffer Overflow (CVE-2015-3955), Insufficient Verification of Data Authenticity (CVE-2015-3956), Uncontrolled Resource Consumption (CVE-2015-3958), Improper Authorization (CVE-2015-3954) and Use of Hard-coded Password (CVE-2015-3953). Five of these vulnerabilities have a high risk level. All but one of these vulnerabilities could be exploited remotely. The Key Management Errors vulnerability could only be used by local users.

For **SCADA** systems the most widespread issues are **cross-site scripting** (seven vulnerabilities), **buffer overflows** (five vulnerabilities), **cross-site request forgery** (four vulnerabilities), **unrestricted file upload** (three vulnerabilities) and **SQL injection** (three vulnerabilities). For instance, a local SQL injection vulnerability (CVE-2015-1008) in Emerson AMS Device Manager before version 13 allows for authenticated users to gain administrative privileges via malformed input.

3.5 Vulnerabilities by Types

The most widespread vulnerability types for ICS components in 2015 are **buffer overflows** (9% of all detected vulnerabilities), use of **hard-coded credentials** (7%) and **cross-site scripting** (7%). The top ten most widespread types of vulnerabilities are presented in Figure 9.

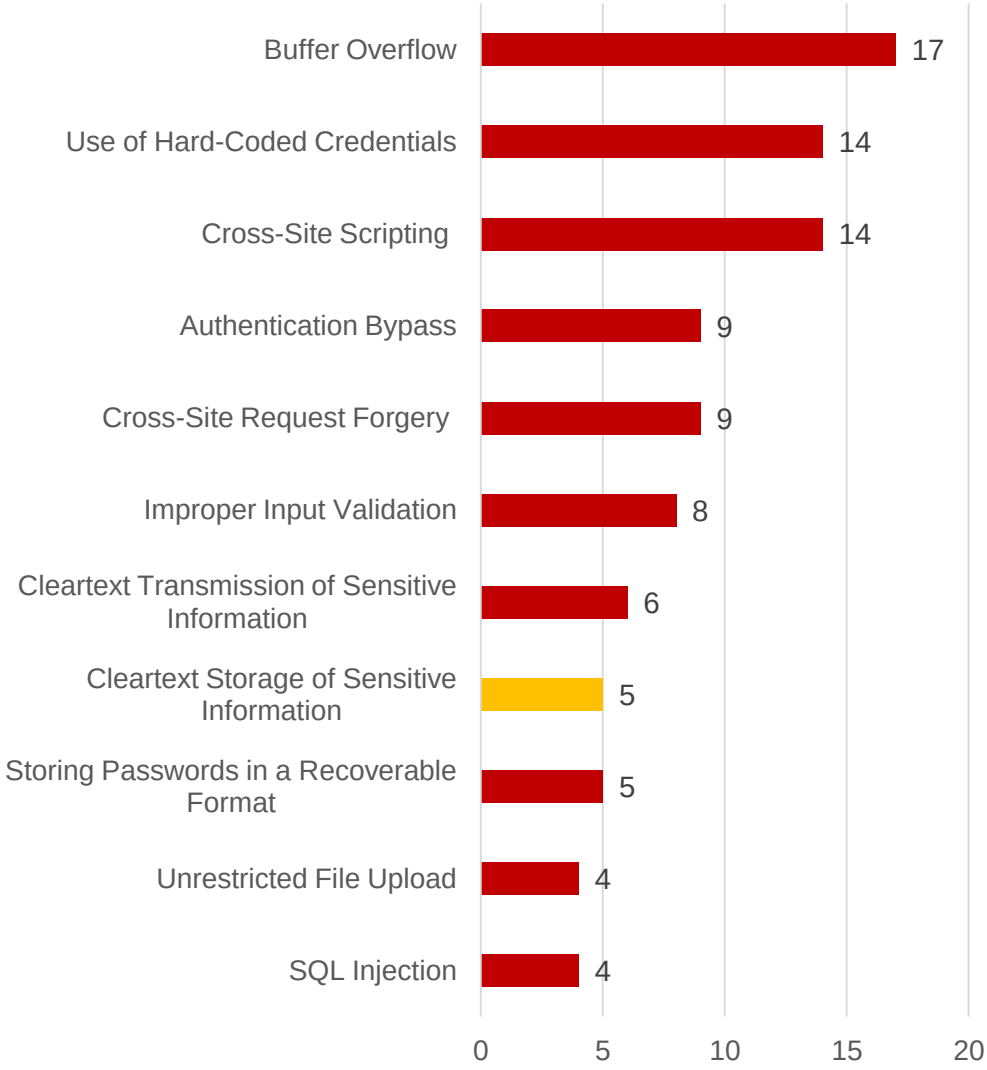

Figure 9. Top 10 vulnerabilities of ICS components in 2015

A **Buffer Overflow** is a programming error, where software, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code. In total, 17 Buffer Overflow vulnerabilities were found in ICS components in 2015, eight of them have a high risk level. These security flaws were discovered in different components, including SCADA systems, HMI, controllers, DCS and others. Four of these vulnerabilities have the highest CVSS score – 10, corresponding to the maximum impact (high-privileged access), which could be done by a remote unauthenticated attacker.

Hard-Coded Credentials, such as a password or cryptographic key, typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator. This vulnerability was discovered in 14 different ICS components (HMI, PLC, Network Devices and others), and in most cases it has a high risk level. Almost all of the identified vulnerabilities of this type could be exploited by a remote attacker. Only one vulnerability (CVE-2015-0996) in Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 can be exploited only by local users.

Cross-Site Scripting enables attackers to inject client-side scripts into web pages viewed by users, which could be used to steal user authentication data (cookies), perform social

engineering attacks, or spread malware. Vulnerabilities of this type are present in 14 ICS components (most of them are SCADA systems).

The Cross-Site Request Forgery vulnerability exists when a web server is designed to receive a request from a client without any mechanism for verifying that it was sent intentionally. Then, it might be possible for an attacker to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This can be done via a URL, image load, XMLHttpRequest, etc. and can result in the exposure of data or unintended code execution. Four of nine vulnerabilities discovered are present in SCADA systems.

Products containing the **Improper Input Validation** vulnerability do not validate, or incorrectly validate, inputs that can affect the control flow or data flow of a program. Most of these flaws are related to arbitrary code execution. Eight vulnerabilities are present in the HMI, SCADA system, RTOS and OPC server. For example, the CVE-2015-0980 vulnerability (high-level) in SCADA Engine BACnet OPC Server before 2.1.371.24 allows an attacker to execute arbitrary code.

Cleartext Transmission of Sensitive Information vulnerabilities were found in six different ICS components. These vulnerabilities allow an unauthorized actor to sniff sensitive or security-critical data in a communication channel because the software transmits data in cleartext. For instance, because there is no SSL support in the Adcon A840 Telemetry Gateway Base Station, all the communication is unencrypted, making it easily readable over the network (CVE-2015-7932, medium-level).

The **Storage of Passwords in a Recoverable Format** makes them subject to password reuse attacks by malicious users. In fact, it should be noted that recoverable encrypted passwords provide no significant benefit over plaintext passwords, since they are subject not only to reuse by malicious attackers, but also by malicious insiders. If a system administrator can recover a password directly, or use a brute force search on the available information, the administrator can use the password on other accounts. HMIs are the most affected by this vulnerability.

Unrestricted File Upload vulnerabilities in software allow an attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. These vulnerabilities were discovered in four ICS components, three of them are SCADA systems. For example, through a servlet, it is possible to upload arbitrary Java code in AggreGate Platform Version 5.21.02 and prior versions, and allow application properties to be imported through uploaded files that could allow arbitrary code and command execution (CVE-2015-7912, high-level).

The basic form of **SQL Injection** describes the direct insertion of attacker-controlled data into variables that are used to construct SQL commands. As a result, an attacker can tamper with the original query by permanently terminating the string, appending new commands etc. Vulnerabilities of this type are present in four ICS components (three of them are SCADA systems).

If information is stored in cleartext **(Cleartext Storage of Sensitive Information vulnerability)**, attackers could potentially read it. Even if information is encoded in a way that is not readable by humans, certain techniques could determine which encoding is being used, and then decode the information. This type of medium level vulnerability is present in different ICS components: HMIs, SCADA systems, Web servers, and pumps.

Authentication Bypass vulnerabilities were found in eight different types of ICS components, including HMI, a network device, RTU and others. An attacker exploiting these vulnerabilities may be able to capture or modify privileged information, inject code, or bypass access control. Depending on a vulnerable system, such flaws can have a different nature,

for example the use of a vulnerable servlet (CVE-2015-6480), a web server allowing an attacker to directly access the information by ignoring the location header (CVE-2015-7910), or incorrect file system architecture (CVE-2015-1599).

Some authentication bypass vulnerabilities are exploitable only under certain conditions:

- A legitimate user must be logged into the web interface Siemens SICAM MIC (CVE-2015-5386).
- Network access to the port 102/TCP is available and the Communication Processor's configuration is stored on its corresponding CPUs (CVE-2015-8214).
- An active web session of an authenticated user exists at the time of attack on Siemens SCALANCE X-200IRT switch (CVE- 2015-1049).

As to vendors, Siemens products are more exposed to Authentication Bypass flaws. Moxa and Yokogawa are often affected by Buffer Overflow vulnerabilities. Other vendors have one or two different types of vulnerabilities (Table 1).

Table 1. Vulnerability distribution by vendor

Vendor	Buffer Overflow	Hardcoded Credentials	Cross-Site Scripting	Authentication Bypass	Cross-Site Request Forgery
Siemens	1	0	1	4	1
Moxa	4	1	1	1	0
Schneider Electric	2	1	1	1	0
Advantech	0	1	1	1	1
Yokogawa	3	0	0	0	0
Hospira	1	2	0	0	0
GarrettCom	0	2	1	0	0
Infinite Automation Systems	0	0	2	0	1
OPTO 22	2	0	0	0	0
Janitza	0	1	0	0	1
SCADA Engine	1	0	0	1	0
Rockwell Automation	1	0	1	0	0
General Electric	0	1	1	0	0
eWON	0	0	1	0	1
XZERES	0	0	0	0	2
Adcon Telemetry	0	1	0	0	0
EasyIO	0	1	0	0	0
IBC Solar	0	0	1	0	0
iniNet Solutions GmbH	1	0	0	0	0
Saia-Burgess Controls	0	1	0	0	0
SMA Solar Technology AG	0	1	0	0	0
Westermo	0	1	0	0	0
Sauter	0	0	1	0	0
3S-Smart Software Solutions GmbH	1	0	0	0	0
Exemys	0	0	0	1	0
Inductive Automation	0	0	1	0	0
Motorola	0	0	0	0	1
Nordex	0	0	1	0	0
Resource Data Management	0	0	0	0	1

4 Conclusion

The automation of industrial processes introduces benefits, but also new vulnerabilities. Although they are designed for critical infrastructures, industrial-sector devices are not secure by default; they contain the same type of vulnerabilities as any other system: including buffer overflows, hardcoded credentials, authentication bypass, cross-site scripting, and many others.

Where protection is concerned, the isolation of critical environments can no longer be regarded as a sufficient security control for ICS. The business requirements of the 21st century often make it necessity to integrate ICS with external systems and networks. In addition, the capabilities, motivations and number of threat actors focusing on ICS environments are increasing. From infected hard drives or USB sticks, to unauthorized connections from ICS networks to the Internet through personal smart phones or modems, and from infected distributive kits obtained from vendors, to a hired insider – all of these methods are available to highly-skilled intruders planning an attack on a physically and logically isolated ICS network.

Nowadays, ICS owners should be aware of modern vulnerabilities and threats, and actively improve the security of their ICS environments based on this knowledge. Here, active vendor support is crucial for the prompt identification and remediation of vulnerabilities in ICS products, as well as for sharing workarounds to protect systems before patches are released.

The current trend of active research in ICS security, the publication of vulnerabilities and the release of patches demonstrates progress in this area. Especially when compared to the previous use of vulnerable systems with no knowledge of the vulnerabilities and dangers involved. However, only the joint efforts of government, vendors, security companies and ICS owners can make this approach possible, improving the practice of protecting production environments on a day-to-day basis.

Contact us at: intelligence@kaspersky.com (Kaspersky Security Intelligence Service)

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy