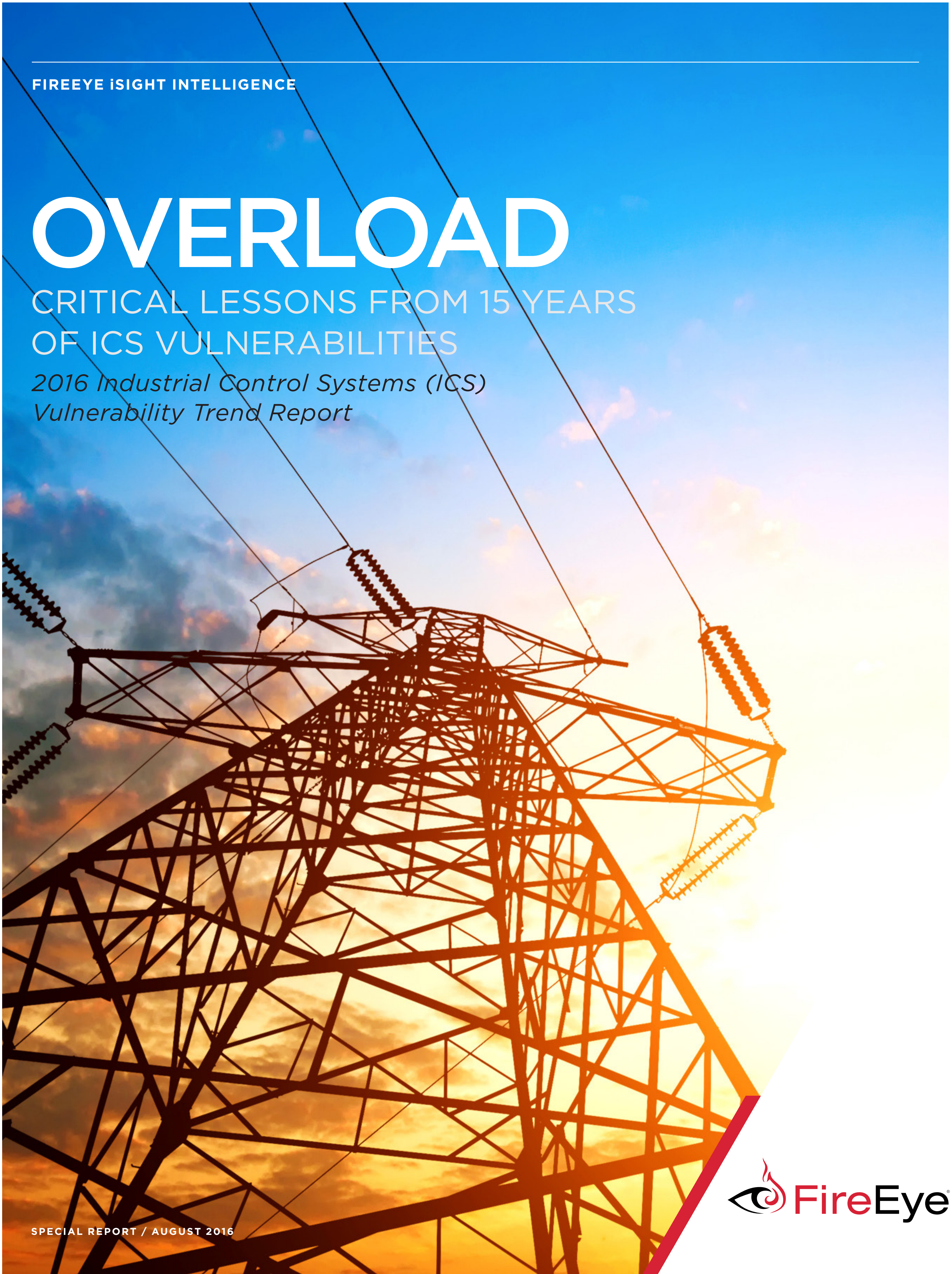
FIREEYE iSIGHT INTELLIGENCE

OVERLOAD

CRITICAL LESSONS FROM 15 YEARS OF ICS VULNERABILITIES

2016 Industrial Control Systems (ICS) Vulnerability Trend Report



SPECIAL REPORT / AUGUST 2016

FireEye

CONTENTS

INTRODUCTION

In the past several years, a flood of vulnerabilities has hit industrial control systems (ICS) — the technological backbone of electric grids, water supplies and production lines. These vulnerabilities affect the reliable operation of sensors, programmable controllers, software and networking equipment used to automate and monitor the physical processes that keep our modern world running.

Since 2000, FireEye iSIGHT Intelligence has identified nearly 1,600 publicly disclosed ICS vulnerabilities. Many of these are unpatched — and some are simply unpatchable due to outdated technology —providing open paths for adversarial exploitation. Nation-state cyber threat actors have exploited five of these vulnerabilities in attacks since 2009.

Unfortunately, security personnel from manufacturing, energy, water and other industries are frequently unaware of their own control system assets, let alone the vulnerabilities that affect them. Organizations operating these systems are missing the warnings and leaving their industrial environments exposed.

This report highlights trends in total ICS vulnerability disclosures, patch availability, vulnerable device type and vulnerabilities exploited in the wild.

KEY JUDGMENTS

The discovery of Stuxnet in 2010 drove **interest in industrial control systems (ICS) vulnerability research**. FireEye iSIGHT Intelligence counted just 149 ICS vulnerability disclosures that were made between January 2000 and December 2010. Through April 2016, we have counted 1,552. We anticipate this upward trend will continue.

58%

Most (58%) of the 801 ICS-specific vulnerability disclosures since February 2013 dealt with Level 2 (L2) in the simplified Purdue ICS architecture model, which describes how manufacturing devices interface with computers. We surmise that this is because L2 software is easier to obtain than L1 devices and is more familiar to a greater number of vulnerability researchers. However, adversary access to L2 alone is generally sufficient for at-will interaction with the controlled process.

Vulnerability patching presents a significant challenge. Of the 1,552 total vulnerability disclosures we examined, 516 (33%) had no vendor fixes. The lack of vendor fixes and slow patch times for most industrial environments presents a significant opportunity for potential adversaries.

Through April 2016, at least five ICS-specific vulnerabilities have been exploited in the wild, **a rate we anticipate will increase in the future**.

In light of these observations and trends, **we recommend that ICS asset owners:**

- Prepare their security teams with an accurate understanding of control system assets, their locations, and functions.
- Obtain structured vulnerability and patch feeds that cover a wide variety of sources.
- Match the vulnerability disclosures and patch announcements against their asset inventory.
- Track vulnerable and unpatched products currently used in their industrial environments.
- Prioritize vulnerability remediation efforts by considering ICS architecture location, simplicity of exploitation and possible impact on the controlled industrial process.

METHODOLOGY

For the purpose of this report, ICS-specific vulnerability disclosures consist of a vulnerability announcement where 1) a disclosing party specifically examined products intended to aid in the operation of an industrial process, and 2) exploitation of the vulnerability has a distinct impact on the controlled industrial process.

- We do not count a disclosure unless it names a specific product.
- We exclude general purpose operating systems, such as Microsoft Windows, even though human machine interfaces (HMIs), engineering laptops and supervisory control and data acquisition (SCADA) servers commonly use them. We also exclude database applications, such as Oracle and SQL Server, even though control system applications and historians commonly incorporate them. Parties disclosing vulnerabilities in these products have not generally done so with ICS in mind.
- By the same reasoning, we excluded major third-party software vulnerabilities/attacks, including POODLE, Heartbleed, and Shellshock, though a variety of ICS-specific software exhibits these issues.
- Further, if a researcher discloses a vulnerability that affects multiple products that have different uses in an industrial environment, and those uses lead to differing impacts on the controlled process, we count them separately. For example, if a researcher discloses a vulnerability in an OPC server (a type of process controller) library the vendor bundles into both a historian and an engineering workstation, we count this as two disclosures because successful exploitation can lead to distinct process impacts.
- Additionally, we have not independently confirmed the accuracy of the disclosures or the efficacy of associated patches.

BY THE NUMBERS

1,552	Number of **ICS SPECIFIC VULNERABILITIES** we analyzed
123	**TOTAL NUMBER OF VENDORS** **affected by vulnerability disclosures**
15	**YEARS OF DISCLOSURES** in our research
33	**PERCENTAGE OF VULNERABILITIES** without a patch at time of disclosure
90	**PERCENTAGE OF VULNERABILITIES** in our data set disclosed after Stuxnet emerged in media reports in mid-2010
465	**NUMBER OF DISCLOSURES** impacting Level 2 of the simplified Purdue model, which typically includes SCADA systems

ICS-SPECIFIC VULNERABILITY DISCLOSURES OVER TIME

STUXNET DROVE INTEREST IN ICS-SPECIFIC VULNERABILITIES

An examination of 1,490 ICS-specific vulnerability disclosures between 2000 and 2015 (see Figure 1) shows a sharp increase in 2011. We believe the media attention garnered by Stuxnet is the principal driver of the increase:

- Stuxnet was the first publicly recognized attack to exploit vulnerabilities in ICS products.[1] Media coverage began in mid-2010 and continued for the next 18 months.
- There was a general slow upward trend prior to 2010, which itself saw just 55 ICS vulnerability disclosures.
- 2011 included 219 ICS vulnerability disclosures, representing a 300% growth from 2010.
- Most (90%) of the vulnerabilities came after 2010, though that accounts for only one-third of the timeline.
- While the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which coordinates vulnerability disclosures between researchers and vendors, formally launched in November 2009, may have had some effect on disclosure rates, we consider that effect secondary because CERT/CC effectively coordinated ICS-specific vulnerability disclosures before that date.

AVERAGE YEARLY DISCLOSURES LIKELY TO INCREASE, BUT NOT AT 2015 RATE

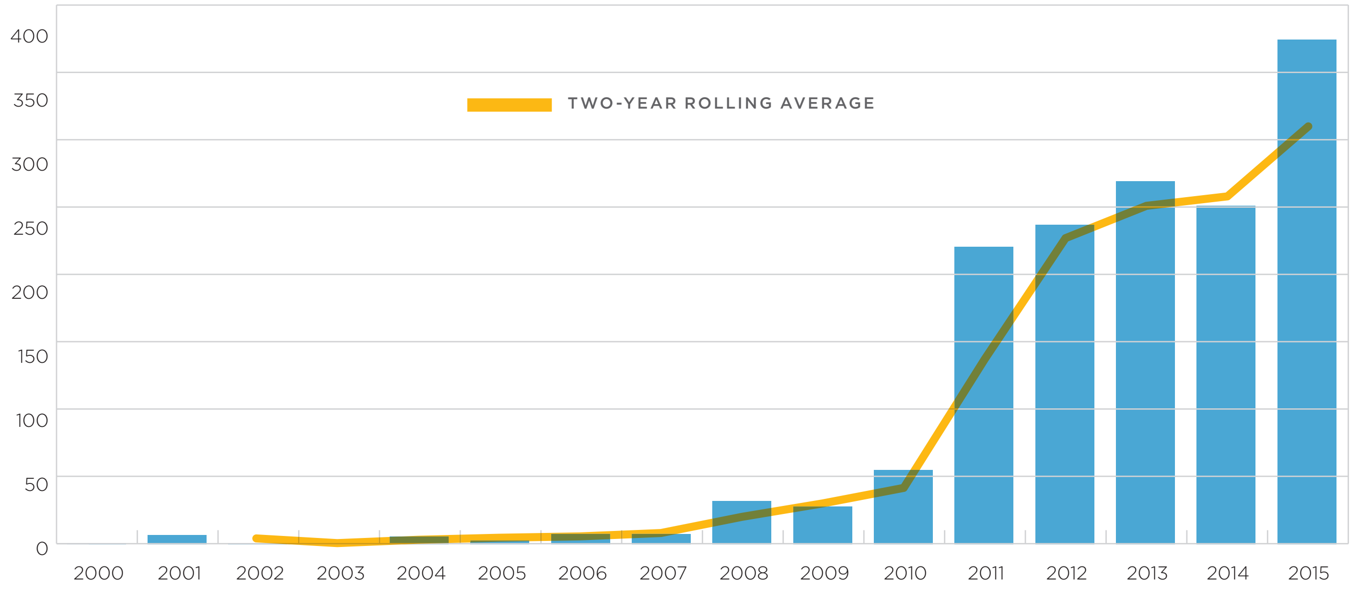
We identify another sharp increase from 2014 to 2015—when disclosures rose from 249 to 371, or by 49%. Prior to this (from 2011 to 2014), disclosures rose an average of just 4.7% annually.

We anticipate that the average number of ICS-specific vulnerability disclosures will increase during the next several years at about the rate it did from 2011 to 2014 (5%) rather than the rate in 2015 (49%).

We surmise that the 2015 increase represents an anomalous spike rather than a new threshold because 92 of the vulnerabilities were caused by two large groups of disclosures that vendors released at a single time: 56 from OSIsoft and 36 from Yokogawa.[2,3]

- The size of these vendor releases are anomalous in the data set. The next largest group of disclosures by a vendor was 12 in 2014.
- Releasing a set of vulnerabilities — versus one-by-one as they are likely discovered — indicates that the vendor may be choosing to address them all at once rather than serially. Vendors may believe that a group and disclose approach enhances marketing of new releases, but we have yet to determine whether this approach is a trend.
- We suggest the Yokogawa vulnerabilities may have been discovered simultaneously because they dealt with similar buffer overflows, but affected multiple products.

FIGURE 1: ICS-SPECIFIC VULNERABILITY DISCLOSURES BY YEAR

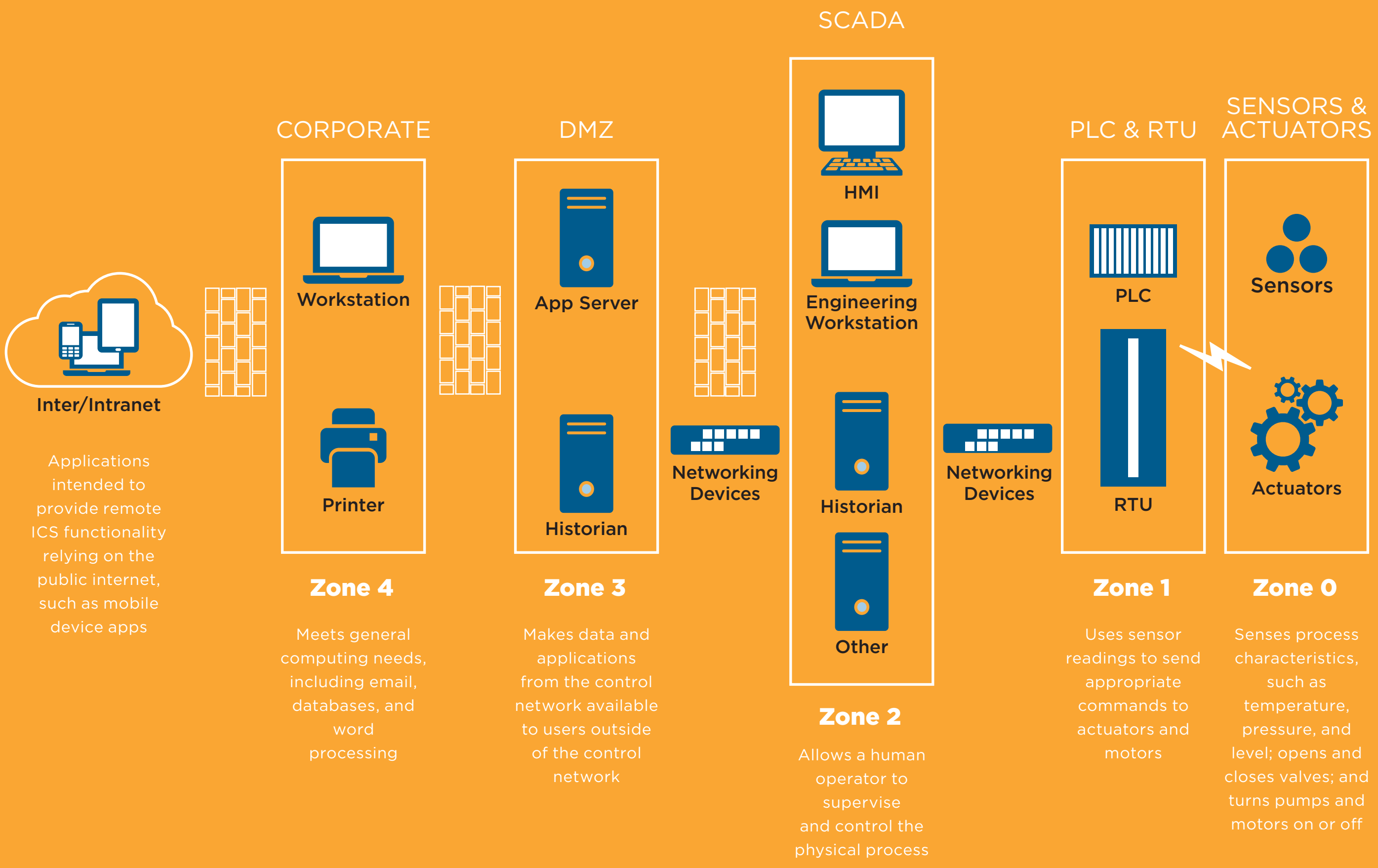


[1] Keizer, Greg. “Is Stuxnet the ‘best’ malware ever?” Infoworld. 16 September 2010. http://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html
[2] OSISoft. OSIsoft Releases Multiple Security Updates for the PI System. 11 August 2015. https://techsupport.osisoft.com/Troubleshooting/Alerts/AL00289.
[3] Yokogawa. Yokogawa Security Advisory Report. 10 September 2015. http://web-material3.yokogawa.com/YSAR-15-0003E.pdf

VULNERABILITIES BY ICS LEVEL

FireEye iSIGHT Intelligence classifies ICS vulnerabilities by their location on a simplified Purdue ICS architectural model.[4] The model (as shown in Figure 2) identifies six levels based on the device's functions and location on the network. We classify industrial networking equipment (normally hardened to withstand harsh temperatures, vibration and dust) in another category.

FIGURE 2: SIMPLIFIED PURDUE MODEL OF AN INDUSTRIAL CONTROL SYSTEM


SCADA
CORPORATE
DMZ
PLC & RTU
SENSORS & ACTUATORS
Inter/Intranet
Applications intended to provide remote ICS functionality relying on the public internet, such as mobile device apps
Workstation
Printer
Zone 4
Meets general computing needs, including email, databases, and word processing
App Server
Historian
Zone 3
Makes data and applications from the control network available to users outside of the control network
Networking Devices
HMI
Engineering Workstation
Historian
Other
Zone 2
Allows a human operator to supervise and control the physical process
Networking Devices
PLC
RTU
Zone 1
Uses sensor readings to send appropriate commands to actuators and motors
Sensors
Actuators
Zone 0
Senses process characteristics, such as temperature, pressure, and level; opens and closes valves; and turns pumps and motors on or off

[4] The Simplified Purdue model refers to a framework developed by researchers to describe the interconnectivity of computers to manufacturing systems.

MOST DISCLOSURES AFFECT LEVEL 2 PROBABLY BECAUSE OF RESEARCHER'S FAMILIARITY WITH THE SYSTEMS AND THE PRODUCT'S AVAILABILITY

About half (465 of the 801 vulnerability disclosures from February 2013 to April 2016) affect products at ICS architecture Level 2 (as shown in Figure 3). We believe Level 2 has received the most attention because:

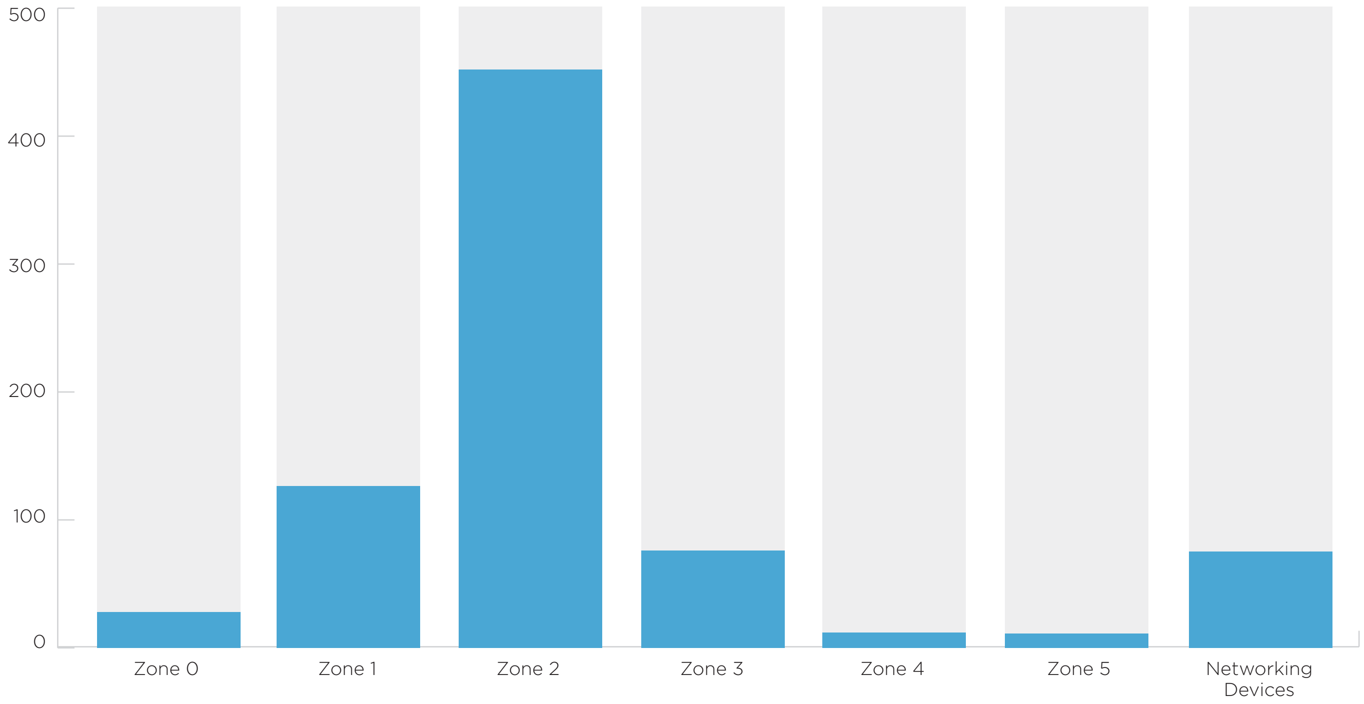
- Equipment in this level frequently relies on operating systems, databases, and other information technologies already familiar to vulnerability researchers; and
- Technologies used at this level can be easily and inexpensively obtained by vulnerability researchers, such as limited-time, full-featured demonstration versions.

ACCESS TO LEVEL 2 ALLOWS A THREAT ACTOR TO MANIPULATE PROCESSES

Once an attacker has unrestricted access to Level 2, further exploits and vulnerabilities become less important because:

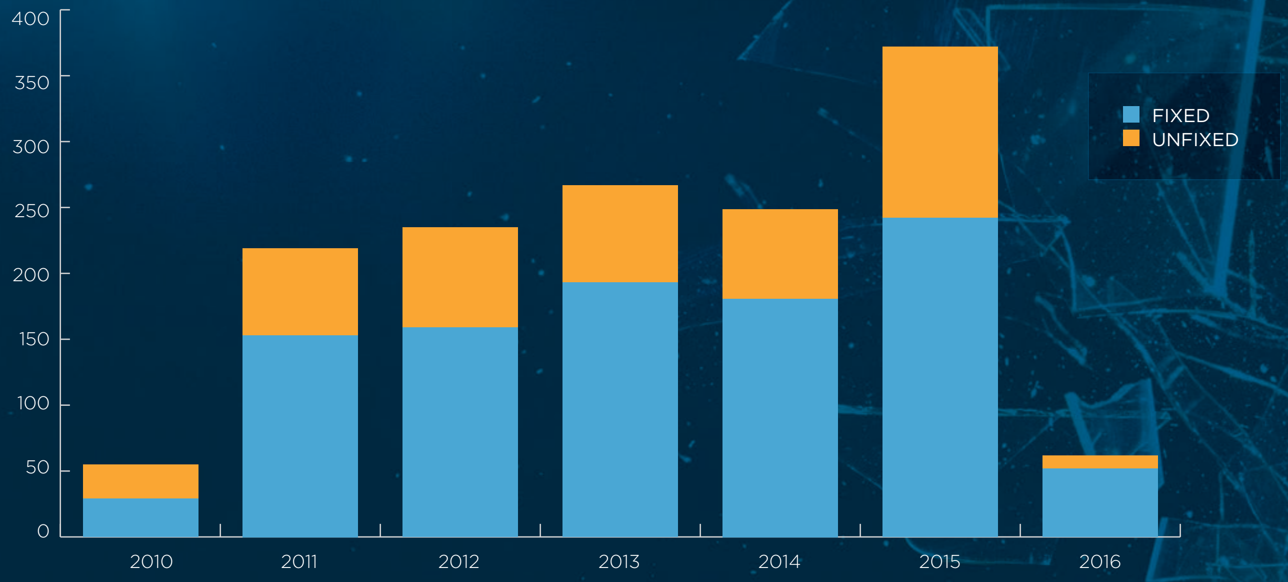
- Devices that directly control the processes, such as HMI and engineering workstations, reside here. Like having a master key, controlling one of those devices gives attackers control of any connected processes. For example, as seen in the attacks on the Ukrainian power companies in December 2014, once attackers have access to the HMI, they can open and close switches and actuators at will without exploiting additional vulnerabilities.
- Using unauthenticated protocols allows any computer connected to these networks to interact with the controlled process. For instance, the use of Modbus/TCP allows any device on the network to alter a set point within the process logic executed by the controller.

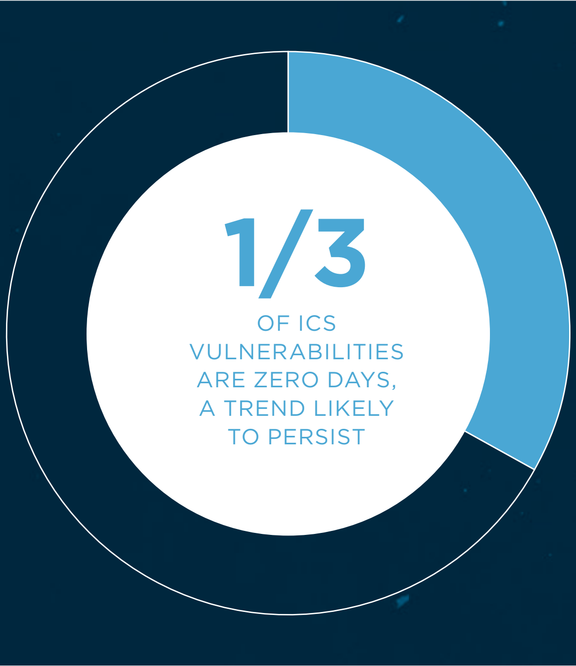
FIGURE 3: ICS-SPECIFIC VULNERABILITY DISCLOSURES AFFECTING EACH LEVEL FROM FEBRUARY 2013 TO APRIL 2016 (VULNERABILITIES MAY AFFECT MORE THAN ONE ZONE)



PATCH AVAILABILITY

FIGURE 4: ICS-SPECIFIC VULNERABILITIES SINCE 2010 SHOWING FIX AVAILABILITY AT TIME





MORE THAN ONE-THIRD OF ICS VULNERABILITIES ARE UNPATCHED AT THE TIME OF DISCLOSURE, A TREND THAT WILL LIKELY PERSIST

Of the 1,552 total vulnerabilities we examined, 516 did not have a fix available at the time of public disclosure (as shown in Figure 4). This means that 33% were zero-day vulnerabilities. While early indications for 2016 appear to depart from this number, we doubt this percentage will change significantly in the near future.

Figure 4 shows ICS-specific vulnerabilities between January 2010 and April 2016 with a fix available at the time of release and illustrates that the portion of disclosures without a fix has remained fairly constant after 2010. We think several factors may be contributing to the lack of patches:

- Researchers did not disclose the vulnerability to the vendor prior to releasing information about it publicly
- Vendors did not respond to researcher in a timely way, prompting the researcher to disclose
- Vulnerabilities could not be (easily) fixed
- Vendors consider vulnerable device end-of-life

ICS VULNERABILITIES EXPLOITED IN THE WILD

While ICS vulnerability disclosures were influenced by Stuxnet, we have not observed a corresponding increase in ICS vulnerability exploitation. We are aware of five ICS-specific vulnerabilities exploited in the wild (as shown in Figure 5). In addition, given the growth in researcher interest, we surmise that many other ICS-specific vulnerabilities have been exploited in the past, but have not been made public.

FIGURE 5: FIVE ICS VULNERABILITIES EXPLOITED IN THE WILD

VULNERABILITY TITLE	ATTACK	KNOWN VICTIMS	EXPLOITED	VULNERABILITY DISCLOSED	PATCH RELEASED
Siemens Simatic S7 DLL loading mechanism vulnerability[5]	Stuxnet	NEDA Industrial Group, Natanz, Iran	July 2009	June 2010	September 2011
Siemens WinCC insecure SQL Server authentication[6]	Stuxnet	NEDA Industrial Group, Natanz, Iran	July 2009	June 2010	July 2012
GE Cimplicity Path Traversal[7,8]	Attributed to the Sandworm Team	Various	January 2012	June 2012	December 2013
Moxa UC-7408-LX Plus unauthenticated firmware[9,10]	Attributed to the Sandworm Team	Kyivo-blenergo Energy Distribution Facility, Ukraine	December 2015	May 2016	Product Discontinued
IRZ RUH2 3G unauthenticated firmware[11]	Attributed to the Sandworm Team	Prykarpattya-oblenergo Energy Distirbution Facility, Ukraine	December 2015	May 2016	N/A

EXPLOITATION OF ICS-SPECIFIC VULNERABILITIES TO ACCRUE AT SLOW RATE

We note that all five instances in which ICS-specific vulnerabilities were exploited can be reasonably tied to nation-state actors. Four of the five — Stuxnet and the attacks in Ukraine — can be tied to direct geopolitical objectives. The success of these incidents in compromising key systems to achieve a political objective or demonstrating an adversary's capabilities makes us expect that nation-state adversaries will increasingly exploit ICS-specific vulnerabilities.

SANDWORM TEAM UNDERMINES THREE UKRAINIAN ELECTRICITY DISTRIBUTORS IN LATE 2015

On Dec. 23, 2015, three Ukrainian electricity distributors found themselves at ground zero for ICS security. A cyber threat group — that we strongly believe is the suspected Russia-based Sandworm Team — had invaded systems and triggered power outages across three regions in western Ukraine.

The attackers systemically shut down the flow of electricity by manipulating distribution system dispatcher HMIs — the applications that grid operators use to control the flow of power to homes and businesses. After shutting down the power, attackers exploited two previously unknown vulnerabilities in control systems networking gear to inhibit the utilities' ability to restore power and maintain control of the grid.

[5] Symanec. "W32.Stuxnet Dossier." February 2011. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. P. 50.

[6] Symanec. "W32.Stuxnet Dossier." February 2011. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. P. 26.

[7] General Electric. "GE Intelligent Platforms Product Security Advisory." 28 October 2014. https://ge-ip.force.com/communities/servlet/fileField?retURL=%2Fcommunities%-2Fapex%2FKnowledgeDetail%3Fid%3DkA21A000000LW4dSAG%26lang%3Den_US%26Type%3DArticle__kav&entityId=ka21A000000PTSeQAO&field=File_1__Body__s.

[8] U.S. Department of Homeland Security. ICS-CERT. "Alert (ICS-Alert-14-281-01E)." 10 December 2014. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[9] U.S. Department of Homeland Security. ICS-CERT. "Advisory (ICSA-16-152-01)." 31 May 2016. https://ics-cert.us-cert.gov/advisories/ICSA-16-152-01.

[10] U.S. Department of Homeland Security." "IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE." 7 March 2016. http://www.eenews.net/assets/2016/07/19/document_ew_02.pdf.

[11] U.S. Department of Homeland Security. "Advisory (ICSA-16-138-01)." 17 May 2016. https://ics-cert.us-cert.gov/advisories/ICSA-16-138-01.

OUTLOOK

In summary, our research supports the following expectations:

- ICS vulnerability disclosures will continue to rise during the coming years at an average close to 5%, with occasional spikes or drops.
- Media coverage of significant events in ICS security, either attacks or research, will likely continue to fuel the vulnerability disclosure rate.
- The majority of disclosures will consist of vulnerabilities affecting Level 2 of the simplified Purdue model.
- While ICS-specific vulnerabilities may not be required to access, manipulate or impact industrial processes, reports of ICS-specific vulnerabilities exploited in the wild will slowly accrue.

RECOMMENDATIONS

The flood of vulnerabilities is likely to overwhelm ICS asset owners as they struggle to keep up with vulnerability notifications, assess associated risk, and implement mitigation. To ensure effectiveness and efficiency in dealing with ICS vulnerabilities, FireEye recommends that ICS asset owners:

- Prepare their security teams with an accurate understanding of control system assets, their locations, and functions.
- Obtain structured vulnerability and patch feeds that cover a wide variety of sources.
- Match the vulnerability disclosures and patch announcements against their asset inventory.
- Track vulnerable and unpatched products currently used in their industrial environments.
- Prioritize vulnerability remediation efforts by considering ICS architecture location, simplicity of exploitation, and possible impact on the controlled industrial process.

To download this or other
FireEye iSight Intelligence reports,
visit: **www.fireeye.com/reports.html**

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye®