NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report

National Cybersecurity and Communications Integration Center/
Industrial Control Systems Cyber Emergency Response Team

Homeland Security

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report.

DHS does not endorse any commercial product or service, including the subject of the analysis in this report. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia, or other visual identities of DHS. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017) and is against DHS policies governing usage of its seal.

EXECUTIVE SUMMARY

This report provides a summary of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) vulnerability coordination activities for FY 2015. The goal of ICS-CERT is to reduce industrial control systems (ICS) risks within and across all critical infrastructure sectors by coordinating efforts among Federal, state, local, and tribal governments, as well as industrial control systems owners, operators, and vendors. ICS-CERT coordinates activities to reduce the likelihood of success and the severity of the impact of cyber-attacks against critical infrastructure control systems.

This report provides trend analysis for all vulnerabilities reported to ICS-CERT in FY 2015. Most notably, researchers found that 52 percent came from improper input validation and permissions, privileges, and access controls. While this high percentage may indicate a pressing cybersecurity gap, it is also possible that it merely reflects the type of vu - nerabilities targeted by researchers reporting to ICS-CERT. The majority of reported vulnerabilities for FY 2015 came from the Energy, Critical Manufacturing, and Water and Wastewater Sectors.

CONTENTS

FIGURES

ACRONYMS

CERT	Computer Emergency Readiness Team
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
NCCIC	National Cybersecurity and Communications Integration Center
US-CERT	United States Computer Emergency Readiness Team

NCCIC/ICS-CERT FY 2015 Vulnerability Coordination Report

1. SCOPE

The intent and scope of this report is to provide a summary of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) vulnerability coordination efforts performed in FY 2015.

2. ICS-CERT VULNERABILITY HANDLING PROCESS

The ICS-CERT vulnerability handling process involves five basic steps:

1. **Detection and Collection:** ICS-CERT obtains vulnerability information in three ways: ICS-CERT vulnerability analysis, monitoring public sources of vulnerability information, and direct notification of vulnerabilities to ICS-CERT by vendors and independent security researchers. After receiving a report, ICS-CERT will perform an initial surface analysis in order to eliminate duplicate reports and false alarms. ICS-CERT then combines and catalogs the remaining vulnerability reports with all private and publicly available information.
2. **Analysis:** Once ICS-CERT has catalogued the vulnerabilities, vendor and ICS-CERT analysts work to understand the vulnerabilities by examining and identifying the issues, as well as the potential threat.
3. **Mitigation Coordination:** After validating a reported vulnerability, ICS-CERT will continue to work with the vendor on mitigation, including possible patch issuance. Researchers then have the opportunity to validate solutions prior to publication.
4. **Application of Mitigation:** ICS-CERT will work with the vendor to allow sufficient time for end users to obtain, test, and apply mitigation strategies prior to disclosure. This time window is variable depending on the circumstances of the vulnerability and the impact to critical infrastructure.
5. **Disclosure:** After gathering the technical and threat information related to the vulnerability, ICS-CERT will notify asset owners about the vulnerability through the publication of an ICS-CERT advisory.

ICS-CERT attempts to coordinate all reported vulnerabilities with the associated vendor. While the goal of ICS-CERT efforts is the timely sharing of vulnerability information, a number of factors may affect the schedule of disclosure. These factors may include the following:

- The severity of the vulnerability,
- Its potential impact to critical infrastructure, public health, and safety,
- The availability of immediate mitigations,
- Whether the information has already been publicly released, and
- The vendor's estimation of time required for the creation, test, and application of a patch or upgrade.

In cases where a vendor is unresponsive, or will not establish a reasonable timeframe for remediation, ICS-CERT may disclose vulnerabilities, regardless of the existence or availability of patches or workarounds from the associated vendors.

3. VULNERABILITY COORDINATION METRICS

This section provides additional detail regarding the development and improvement of ICS-CERT capabilities in FY 2015, including total vulnerability reports, key researchers, and time from vulnerability identification to the successful closure of vulnerability reports.

3.1 Vulnerability Reporting and Resolution

ICS-CERT receives vulnerability reports from vulnerability researchers, industrial control system (ICS) vendors, and national Computer Emergency Readiness Team's (CERT). ICS-CERT opens a ticket when someone reports a vulnerability. ICS-CERT serves as the facilitator between vulnerability researchers and the associated vendor. After the opening of a ticket, vendors will typically validate the vulnerability and create a patch or other mitigations, which the researcher may then validate. After validation of the mitigation, vendors will distribute the patch to their customers. ICS-CERT will not release an advisory describing the vulnerability until after the vendor's customers have been given time to patch their systems (this period is known as a "patch window"). If appropriate, ICS-CERT will publish an alert before the vendor has released a mitigation. For example, if someone has already released information about the vulnerability ICS-CERT will publish an alert before the patch window. After a patch window has expired or, alternatively, if it is evident that the vendor will not provide mitigation, the ticket is closed ("resolved").

Advisories provide timely information about current security issues, vulnerabilities, and exploits. An ICS-CERT advisory is intended to provide awareness to or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activities with the potential to impact critical infrastructure computing networks. An advisory contains information from the researcher's initial report, validation of the vulnerability, a description of the vulnerability including exploitation impact, and mitigations steps that asset owners can apply. ICS-CERT issues an advisory after the vulnerability coordination process has occurred. This means the researcher has contacted ICS-CERT before issuing a public notification of their findings.

ICS-CERT intends for its alerts to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks. ICS-CERT produces alerts based on a vulnerability discovery and the vendor's validation and uses them to rapidly disseminate information about a vulnerability that someone has publicly released without coordination.

In 2015, ICS-CERT produced 197 advisories with 22 initially published to the United States Computer Emergency Readiness Team (US-CERT) Portal and 16 alerts with four initially published to the Portal. Figure 1 shows the number of alerts and advisories published by ICS-CERT from FY 2010 through FY 2015, and Figure 2 shows the number of tickets resolved for the same period.

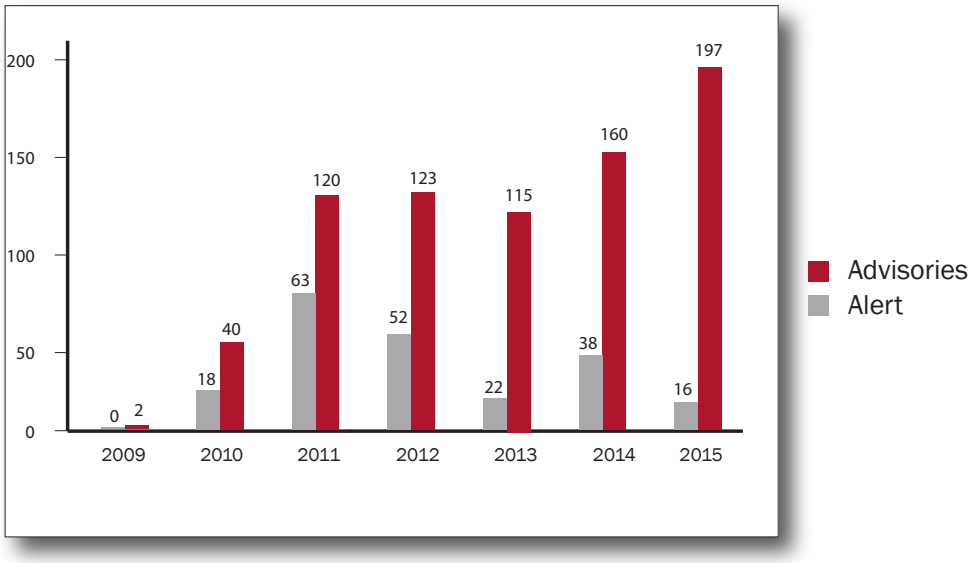

Figure 1. Number of alerts and advisories published by ICS-CERT from FY 2010 through FY 2015.

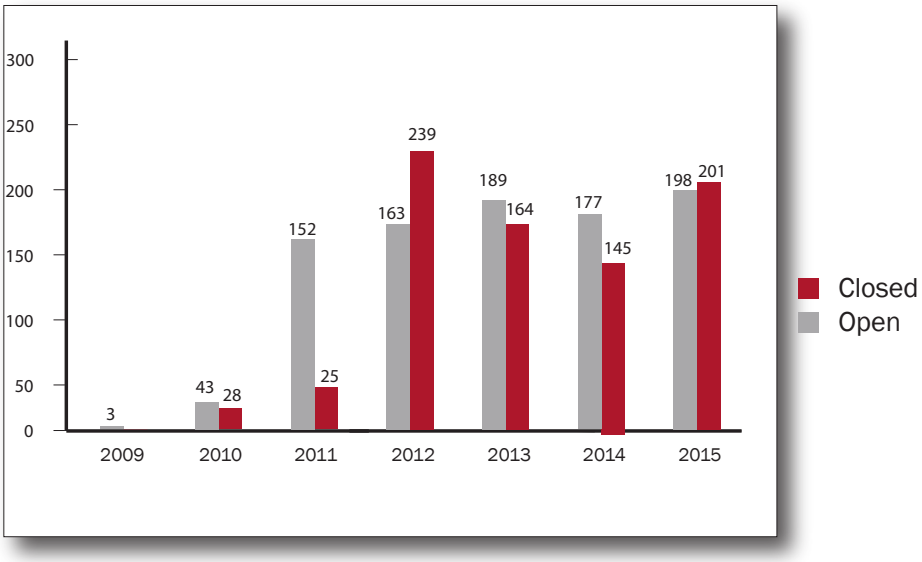

Figure 2. Number of tickets created and resolved by ICS-CERT from FY 2010 through FY 2015.

The increase in the number of vulnerabilities reported is significantly la ger than the tickets created. The disparity is a result of researchers conducting an in-depth assessment prior to submitting a vulnerability report. In the course of its work, ICS-CERT may create tickets that it later merges or eliminates because of issues of applicability. Figure 3 shows the number of ICS vulnerabilities reported to ICS-CERT in FY 2015.

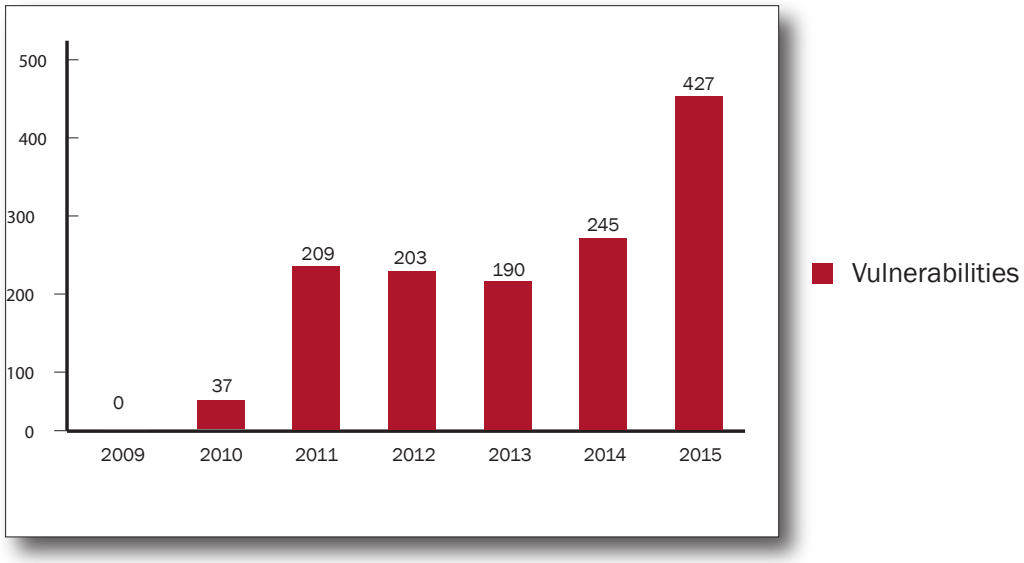

Figure 3. Number of vulnerabilities reported to ICS-CERT 2009 through FY 2015.

Independent researchers report vulnerabilities directly to ICS-CERT, which helps coordinate communications between the researcher and vendor. As previously mentioned, ICS-CERT will not publish an advisory with vulnerability details until the vendor has released a fix to its customers. The following figures display the length of time from when ICS vendors received notification of vulnerabilities unti their tickets were resolved (Figure 4).

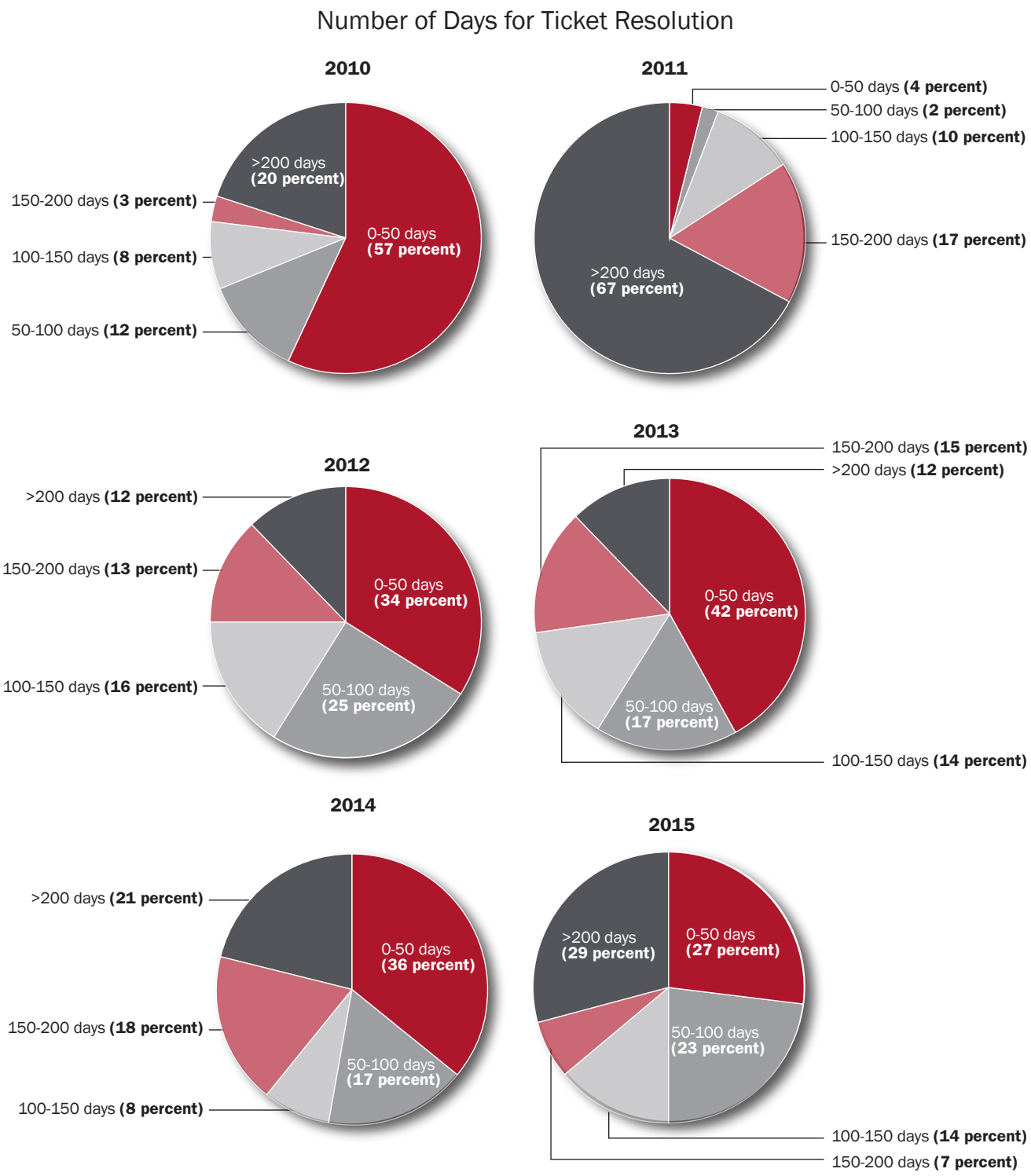

Figure 4. Length of time for ticket resolution.

One of the main goals for 2015 was to reduce the number of tickets that had been open for longer than 365 days. The Vulnerability Coordination Team closed 35 tickets older than 365 days in FY 2015. This represents 76 percent of the tickets open for over 365 days. This success is attributable to elevating the visibility of the vulnerability to the vendor's management level.

3.1.1 Coordinated Disclosure Trends

Some vulnerability researchers publish vulnerabilities without giving the vendor a chance to provide mitigation to its customers. The general trend, however, is that more ICS vulnerability researchers are waiting to publish vulnerabilities that could impact critical infrastructure until the vendor has had an opportunity to mitigate them. Figure 5 shows the percentage of vulnerabilities coordinated with ICS-CERT from FY 2010 to FY 2015.

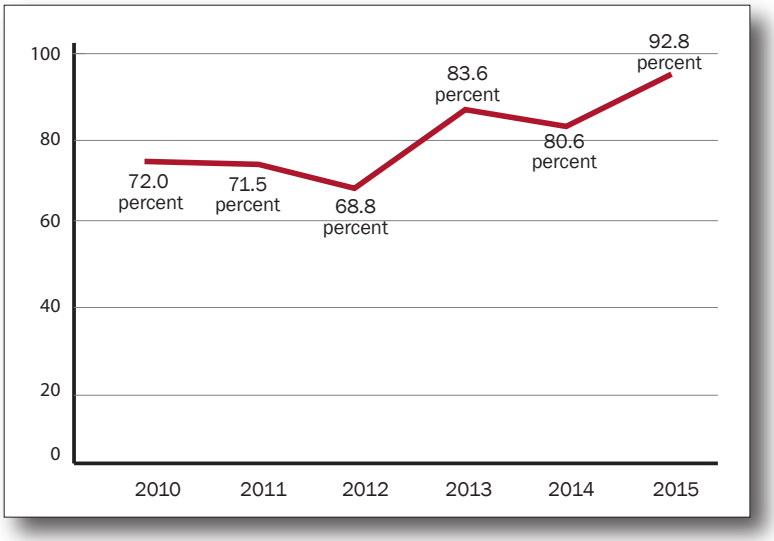

Figure 5. Trend of ICS vulnerabilities coordinated with the ICS-CERT.

3.1.2 Researcher Trends

Independent vulnerability researchers report most ICS vulnerabilities to ICS-CERT, although some report to third-party collaborators, such as the Zero Day Initiative. In addition, ICS-CERT collaborates with international and private sector CERTs, such as the Japan CERT, ICST (Taiwan National Information and Communication Taskforce), and Siemens ProductCERT. The vulnerability researchers who have reported the most vulnerabilities in FY 2015 to the ICS-CERT are listed below:

- Rupp, Maxim 28
- Sanchez, Ivan 13
- Bolshev, Alexander 11
- Sood, Aditya K 10
- Darshanam, Praveen 7
- Ganeshen, Karn 6
- Wightman, Reid 4
- Jartelius, Martin 3

Only three independent researchers from previous years have submitted vulnerabilities in FY 2015:

- Rios, Billy;
- Crain, Adam; and
- Brown, Jeremy.

Some ICS vendors have identified and self-reported vulnerabilities in their own products. The following vendors are ranked in order of vulnerabilities they self-reported in FY 2015:

1. Siemens ProductCERT,
2. GE,
3. Schneider Electric, and
4. OSIsoft.

4. SEVERITY OF ICS VULNERABILITIES

The security industry standard for scoring the severity of a vulnerability is the Common Vulnerability Scoring System (CVSS). ICS-CERT gives vulnerabilities a CVSS score to help asset owners assess the risk a given vulnerability poses to their organization. Figure 8 shows the percentage of ICS vulnerabilities with low, medium, and high CVSS scores. Figure 7 shows that the average CVSS scores reported to ICS-CERT dropped from 8.50 in FY 2010 to 6.85 at the end of FY 2015.

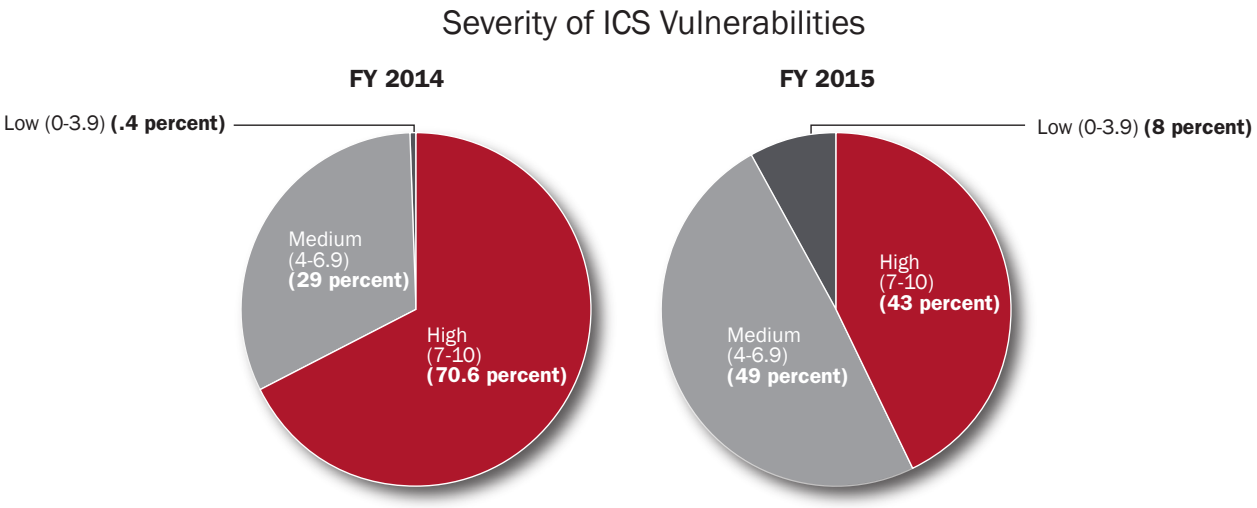

Figure 6. Percentages of ICS vulnerabilities with high, medium, and low CVSS severity scores.

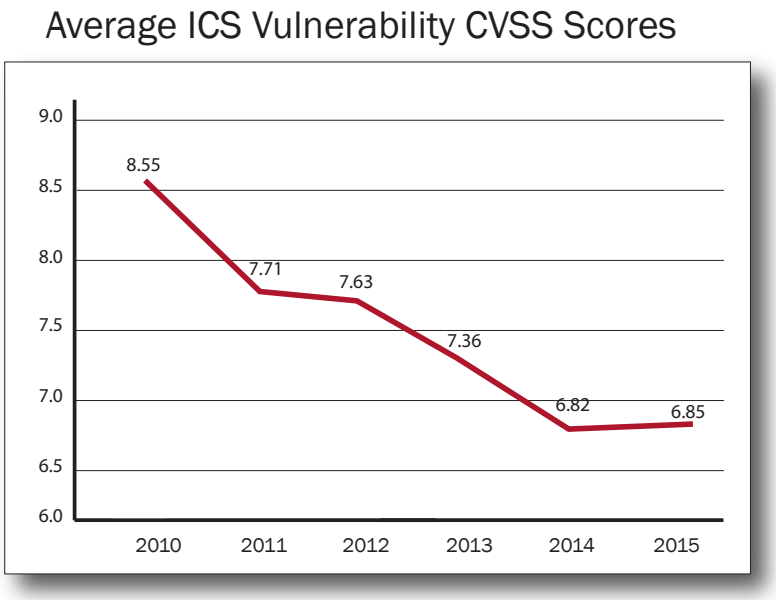

Figure 7. Trend of ICS vulnerability CVSS scores.

4.1 Sectors that Use Products that Have Vulnerabilities Reported to ICS-CERT

Figure 8 displays the sectors where ICS products with reported vulnerabilities are used by fiscal yea . Of the vulnerabilities reported to ICS-CERT, the majority are in products used by the energy, critical manufacturing, and water and wastewater systems sectors.

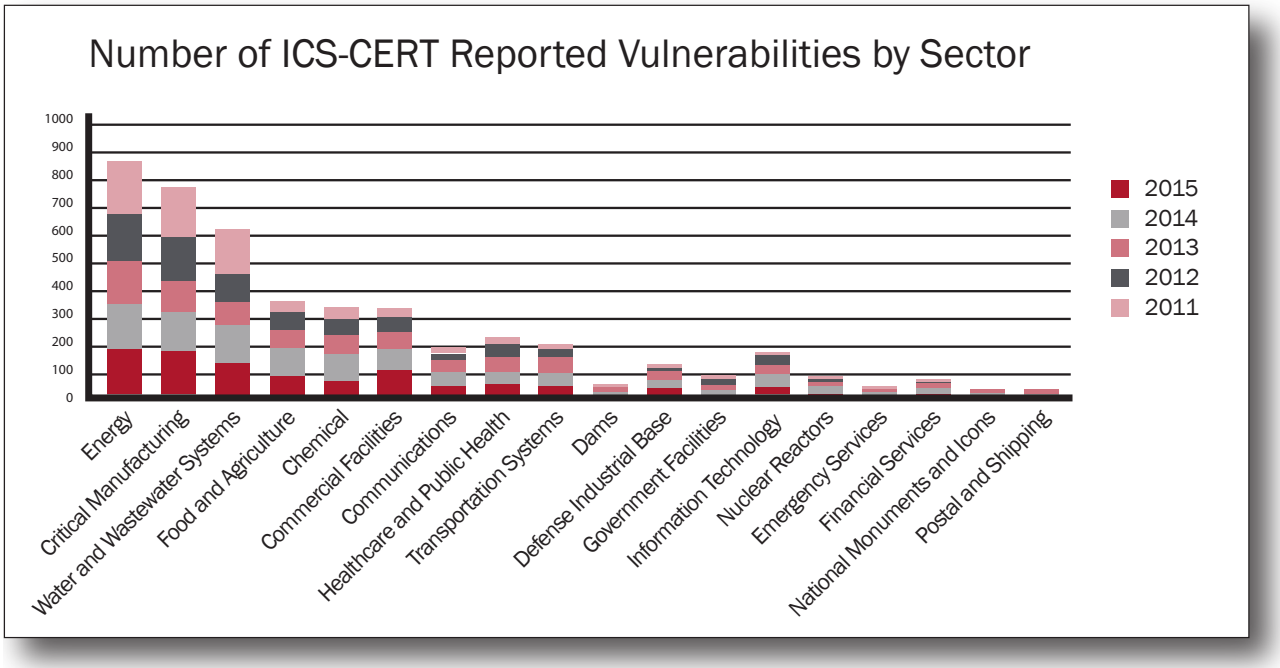

Figure 8. Number of vulnerabilities reported to ICS-CERT in products used in each critical infrastructure sector.

5. TYPES OF VULNERABILITIES REPORTED TO ICS-CERT

Figure 9 shows high-level categories of all vulnerabilities reported to ICS-CERT for FY 2010 through FY 2015. The changes from previous years show an increase in all types with the exception of improper input validation.

Improper input validation vulnerabilities occur when software does not validate input properly; an attacker is able to craft the input in a form that is not expected by the rest of the application. This can lead to parts of the system receiving unintended input, which may result in altered control flo , arbitrary control of a resource, or arbitrary code execution.

Permissions, privileges, and access control is when an authorization policy is defined, individual or sets of users are defined, and applications or processes that can perform actions on a resource such as a database are defined. This can be very granular with an authorization policy. Administrators can control certain actions, such as whether individuals or groups can read, create, modify (write), or delete.

Improper control of a resource vulnerabilities occur when the software does not maintain, or incorrectly maintains, control over a resource throughout its lifetime of creation, use, and release.

Credentials management is a broad administrative area that deals with identifying individuals in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

Indicator of poor code quality vulnerabilities occur when the code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

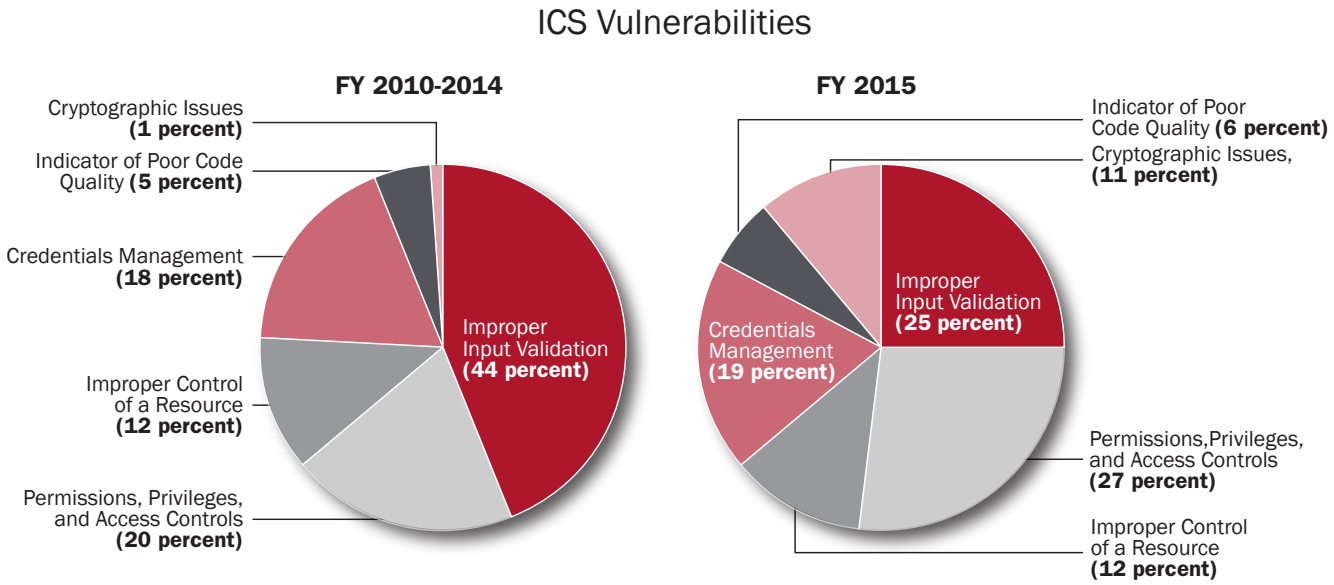

Figure 9. Categories of all vulnerabilities reported to ICS-CERT.

Figure 10 presents the trend of vulnerability types reported from FY 2010 to FY 2015. The increase in reported vulnerabilities corresponds with a significant increase in improper input validation vulnerabil - ties. Figures 11 through 15 compare various vulnerabilities for FY 2010–2015.

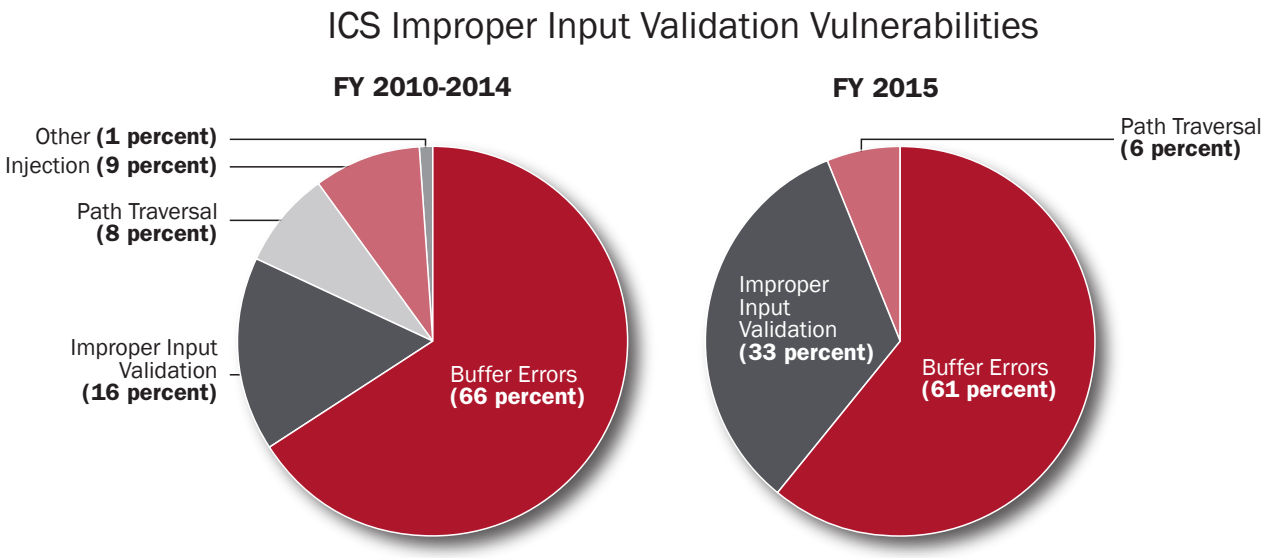

Figure 10. Types of input validation vulnerabilities reported to ICS-CERT.

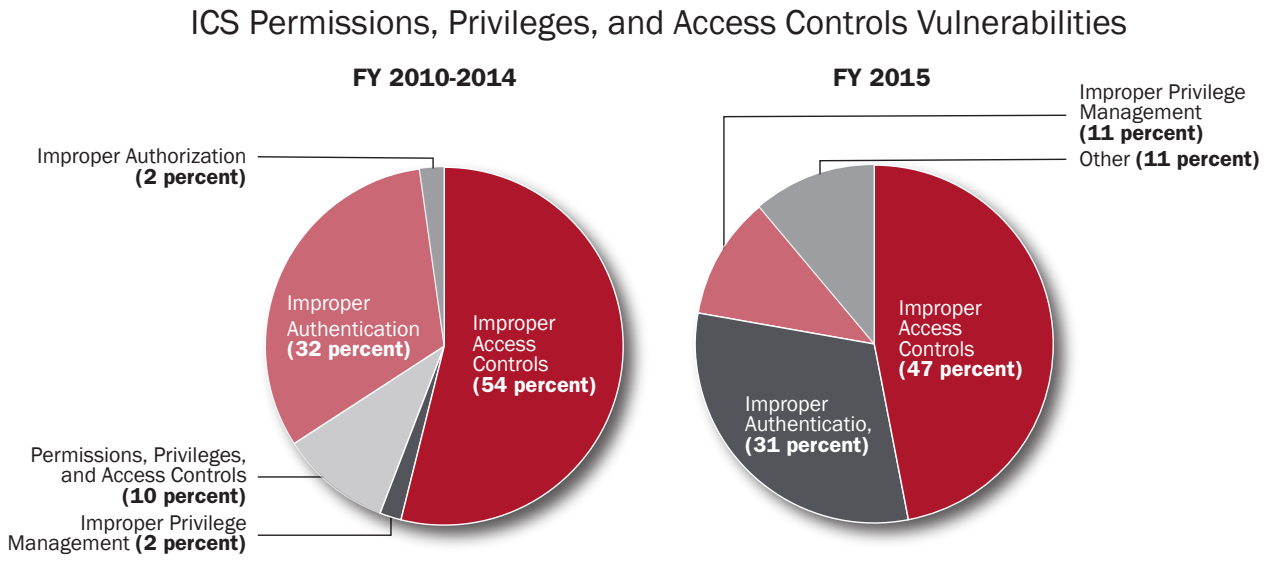

Figure 11. Types of ICS permissions, privileges, and access control vulnerabilities.

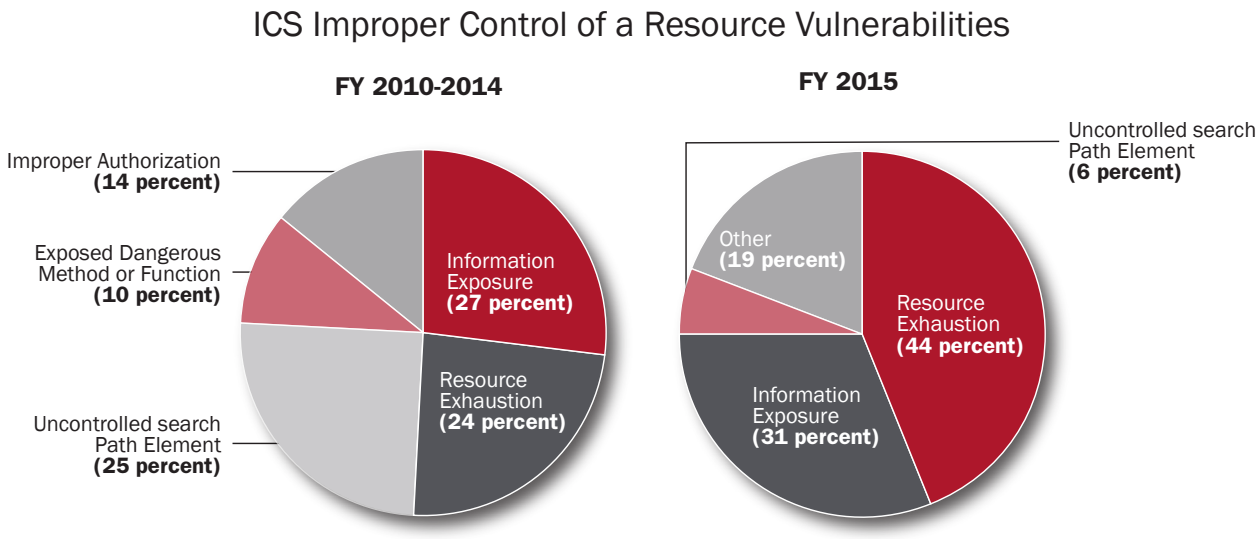

Figure 12. Types of ICS improper control of a resource vulnerabilities.

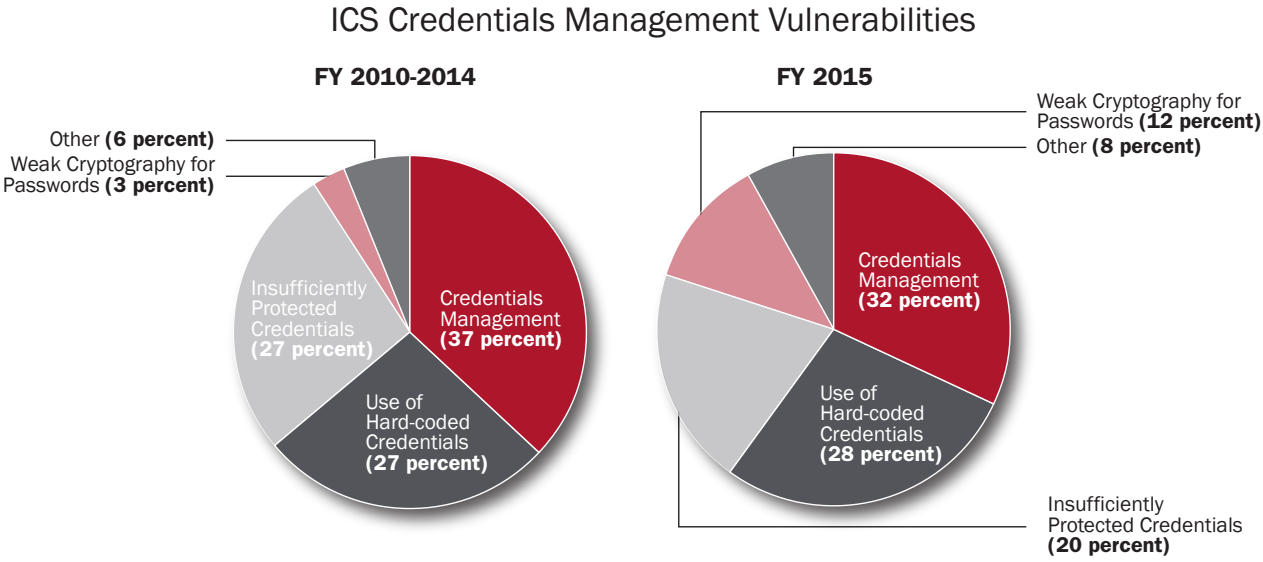

Figure 13. Types of ICS credentials management vulnerabilities, 2010-2013.

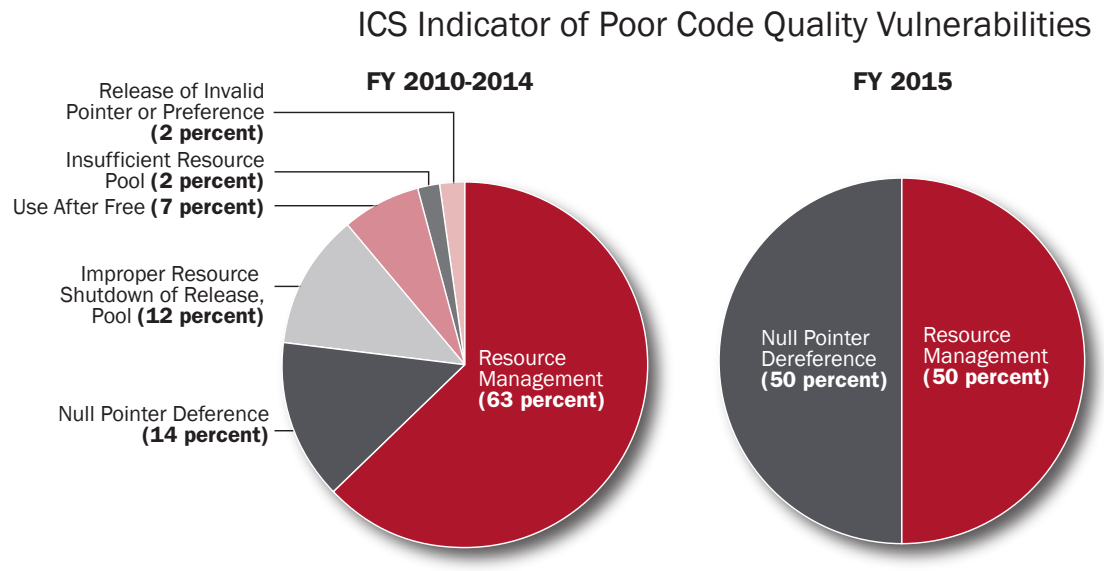

Figure 14. Types of ICS vulnerabilities due to poor code quality.

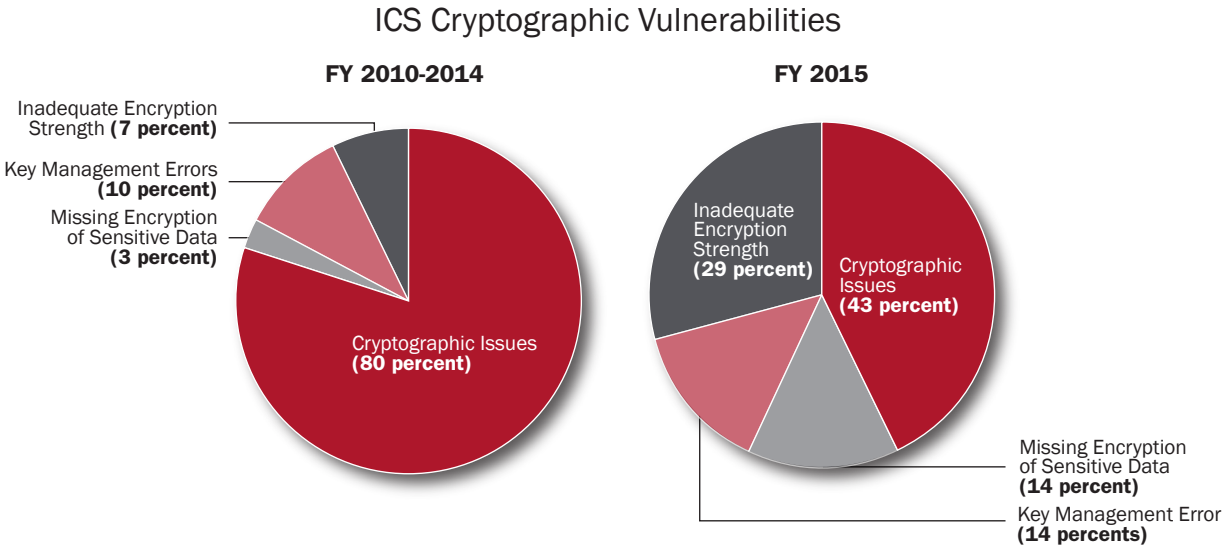

Figure 15. Types of ICS cryptographic vulnerabilities reported to ICS-CERT.

6. CONCLUSION/SUMMARY

Since its establishment, ICS-CERT has actively worked toward improving and enhancing cybersecurity postures within the ICS community by sharing control systems-related security incidents and mitigation measures. During this time, the group has become more effective and efficient sharing threat information and coordinating vulnerability alerts with researchers, vendors, and the ICS community at large.

As the ICS community continues to adopt new technology, it is imperative that public and private partnerships continue to work toward the improved situational awareness of the community as a whole. ICS-CERT urges organizations and asset owners to continue to monitor ICS-CERT advisories and alerts and implement mitigation strategies that will improve the cybersecurity of the nation's critical infrastructure.

Department of Homeland Security

Office of Cybersecurity and Communication

National Cybersecurity and Communications Integration Center

1-888-282-0870

Industrial Control Systems Cyber Emergency Response Team