ICS-CERT Annual Vulnerability Coordination Report

Industrial Control Systems Cyber Emergency Response Team

2016

NCCIC

NCCIC

Table Of Contents

EXECUTIVE SUMMARY

This report summarizes the National Cybersecurity and Communications Integration Center (NCCIC)/ Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) vulnerability coordination activities for Fiscal Year (FY) 2016 and Calendar Year (CY) 2016. NCCIC is a division of the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C). ICS-CERT's Vulnerability team supports cybersecurity efforts across the industrial controls systems (ICS) community by working with its partners to identify, validate, mitigate, and disclose ICS vulnerabilities. The information in this report provides insight into vulnerability trends in 2016 and enhances visibility into ICS-CERT's coordination efforts.

ICS-CERT received 2,282 reported vulnerabilities in FY 2016, which resulted in the release of 157 advisories and 17 alerts. In CY 2016, ICS-CERT received 2,328 reported vulnerabilities, which resulted in the release of 185 advisories and 17 alerts. ICS-CERT analyzed a subset of the total number of vulnerabilities reported in FY and CY 2016 and determined that the average Common Vulnerability Scoring System (CVSS) score for reported vulnerabilities was 7.8/10 and that the four most frequently occurring vulnerabilities types were Stack-based Buffer Overflow, Improper Input Validation, Cross-site Scripting, and Heap-based Buffer Overflow vulnerabilities. In FY and CY 2016, ICS-CERT coordination with product vendors resulted in product fixes for 92.1 percent and 89.3 percent of reported vulnerabilities, respectively. The majority of the vulnerabilities coordinated by ICS-CERT in 2016 were most commonly associated with the Energy, Critical Manufacturing, Commercial Facilities, and Water and Wastewater Systems Sectors.

NCCIC

1. SCOPE

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 efforts performed during Fiscal Year (FY) and Calendar Year (CY) 2016. These coordination efforts apply to all of the 16 critical infrastructure (CI) sectors, as identified in Presidential Policy Directive 21 (PPD-21).

ICS-CERT stood up the Vulnerability Coordination team in response to a recognized need for a single resource to collect, coordinate, and provide vulnerability information to the industrial controls systems (ICS) community. The primary objective of ICS-CERT's vulnerability coordination work is to help mitigate cybersecurity vulnerabilities quickly to reduce the likelihood of a successful cyber attack against the Nation's CI. Vulnerability coordination requires technical expertise, documentation, and close trusted partnerships with key ICS community stakeholders, including vendors; manufacturers; integrators; CI owners; researchers; federal, state, and local government organizations; and international partners.

2. ICS-CERT VULNERABILITY COORDINATION PROCESS

ICS-CERT manages the vulnerability coordination process in five phases:

1. **Vulnerability Identification:** ICS-CERT typically obtains vulnerability information from security researchers and product vendors and by monitoring public sources of vulnerability information. Once ICS-CERT identifies a vulnerability, ICS-CERT reviews it and creates a vulnerability ticket.
2. **Vendor Notification and Validation:** ICS-CERT passes the identified vulnerability to the responsible vendor to validate it and to start the coordination process.
3. **Vulnerability Mitigation:** Following the validation of an identified vulnerability, ICS-CERT provides recommendations and offers assistance while the affected vendor develops and implements a mitigation plan.
4. **Disclosure:** In coordination with the reporting researcher and the product vendor, ICS-CERT releases an information product to notify asset owners and operators about the identified vulnerability and the proposed mitigations. If the vendor needs additional time to communicate with its customers about product fixes, all involved parties negotiate a patch window. The patch window includes the initial release of a portal advisory to the Homeland Security Information Network (HSIN) portal for a predetermined length of time, prior to its public release.
5. **Finalization:** Following the publication of the ICS-CERT information product, the vulnerability team adds any final details to the vulnerability ticket and closes it out.

3. VULNERABILITY METRICS REPORTING CHANGES

The method used to collect and report vulnerability data changed in 2016 from that used in prior years. In 2016, ICS-CERT began reporting metrics data on vulnerability tickets closed within the FY or CY accounting periods. This prevents reported metrics changing based on work accomplished throughout the life of an open ticket. In previous year's reporting methods, actions taken prior to ticket closure could result in additional follow-on work being required, which in turn could change the reported metrics. It is therefore important to note that some information reported in published alerts and advisories in 2016 may not be included in the FY or CY data cited herein, since the associated vulnerability ticket may still be open. Data for tickets will be included in the reporting period in which the ticket is closed.

ICS-CERT provides historical data in this document for the reader's use; however, due to the data collection and reporting changes in 2016, the reader should be cautious in comparing metrics from 2016 with metrics from prior years.

4. INFORMATION PRODUCTS RELEASED

ICS-CERT releases alerts and advisories to notify the ICS community about vulnerabilities that threaten the Nation's CI. Alerts and advisories provide actionable information about known vulnerabilities, threats, and mitigations. This information helps asset owners and operators understand how attackers might compromise their ICS and how to take action to protect their ICS.

ICS-CERT alerts provide timely notification to CI owners and operators about publicly known threats that have the potential to affect ICS. ICS-CERT typically releases alerts soon after the identification of publicly available vulnerability information or exploits. Alerts also provide baseline mitigations to reduce the risk of exploitation.

ICS-CERT advisories provide information about security vulnerabilities in products used in CI and typically contain vendor recommended mitigations or compensating controls.

Table 1 summarizes the number of alerts and advisories for FY and CY 2016. Figure 1 shows historical numbers for alerts and advisories since FY 2010. The graphic does not include calendar year data for years prior to 2016. Because of the change in reporting metrics in 2016, readers should use caution in comparing prior data with that of 2016.

Year	Alerts	Alerts released to HSIN portal	Advisories	Advisories released to HSIN portal[1]
FY 2016	17	5	157	17
CY 2016	17	5	185	14

Table 1. Alerts and advisories released during FY and CY 2016, based on closed tickets.

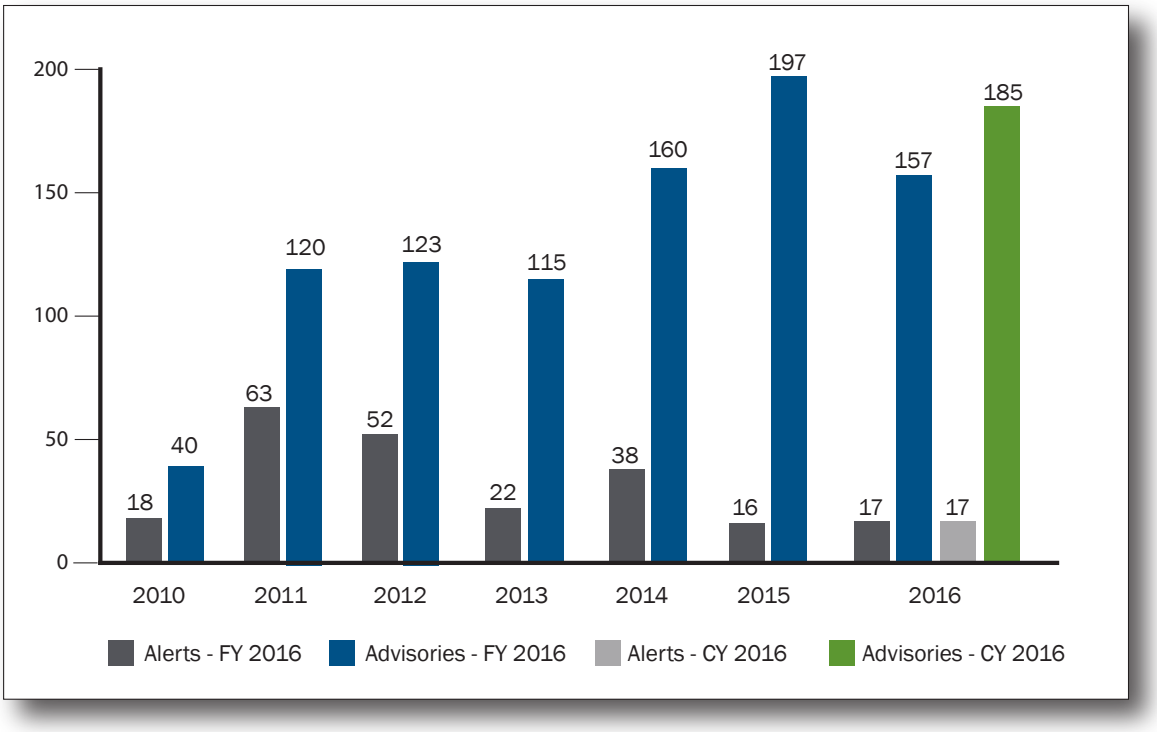

Figure 1. Alerts and advisories released since FY 2010. FY and CY 2016 based on closed tickets.

[1]As mentioned in Section 2 "Disclosure", an alert or advisory released to the HSIN portal is a result of a vendor needing additional time to communicate with their customers about product fixes.

5. OPENED AND CLOSED TICKETS

When ICS-CERT receives a vulnerability report, the Vulnerability team opens (creates) a ticket to track the vulnerabilities associated with the received report. Tickets include information that describes the problem, tracks progress on active steps, maintains contact information, and annotates activities performed for closure.

Table 2 shows the total number of tickets opened and the total number of tickets closed during FY and CY 2016.

Year	Tickets Opened	Tickets Closed
FY 2016	186	143
CY 2016	255	162

Table 2. Vulnerability tickets opened and closed during FY and CY 2016.

Figure 2 shows historical numbers of opened and closed tickets since FY 2010. The graphic does not include calendar year data for years prior to 2016. The slight color differences in Figure 2 for 2016 opened and closed tickets merely reminds the reader of the reporting process change in 2016.

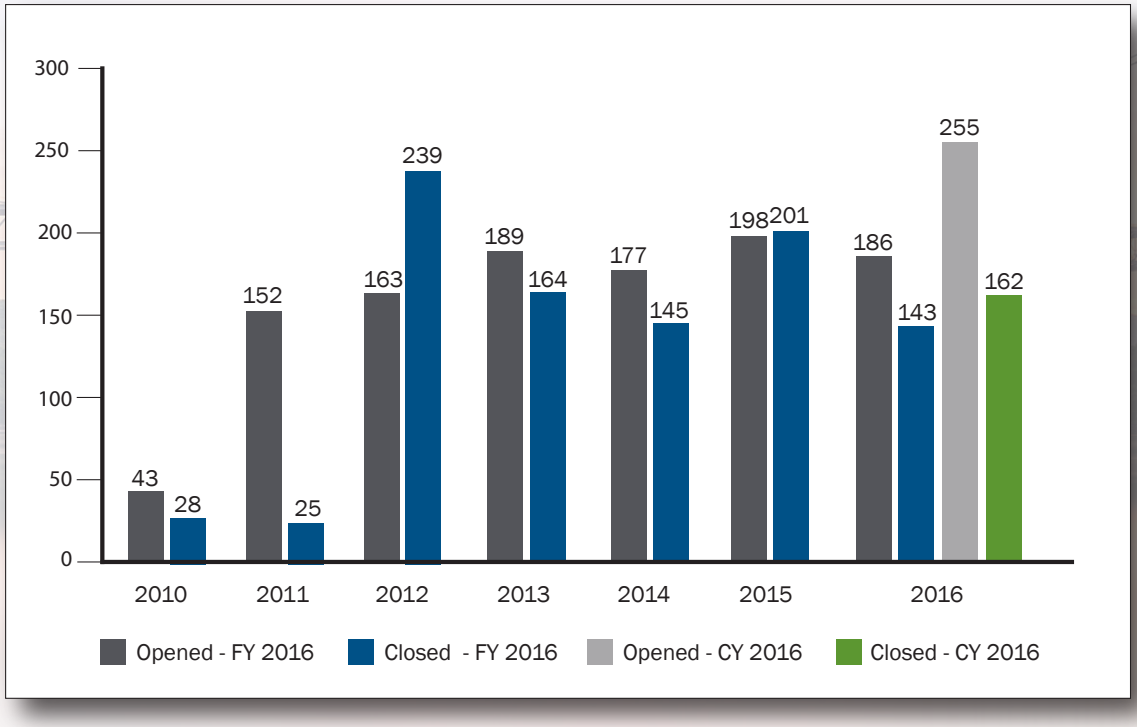

Figure 2. Opened tickets and closed tickets since FY 2010.

6. REPORTED AND COORDINATED VULNERABILITIES

In FY 2016, ICS-CERT coordinated 2,272 vulnerabilities. This number is significantly greater than the number of vulnerabilities reported in prior years. The dramatic increase is primarily due to two vulnerability reports containing hundreds of vulnerabilities, identified by using automated scanning tools.[2] The scanning tools expedite the detection process and make it easier to detect out-of-date third-party software.

Figure 3 shows the total number of vulnerabilities reported to ICS-CERT prior to FY 2016, as well as the number of vulnerabilities coordinated by ICS-CERT in FY and CY 2016. The graphic does not include calendar year data for years prior to 2016. With the metrics reporting change in 2016 to using closed tickets, ICS-CERT advises caution when comparing data from FY 2016 with data from prior years.

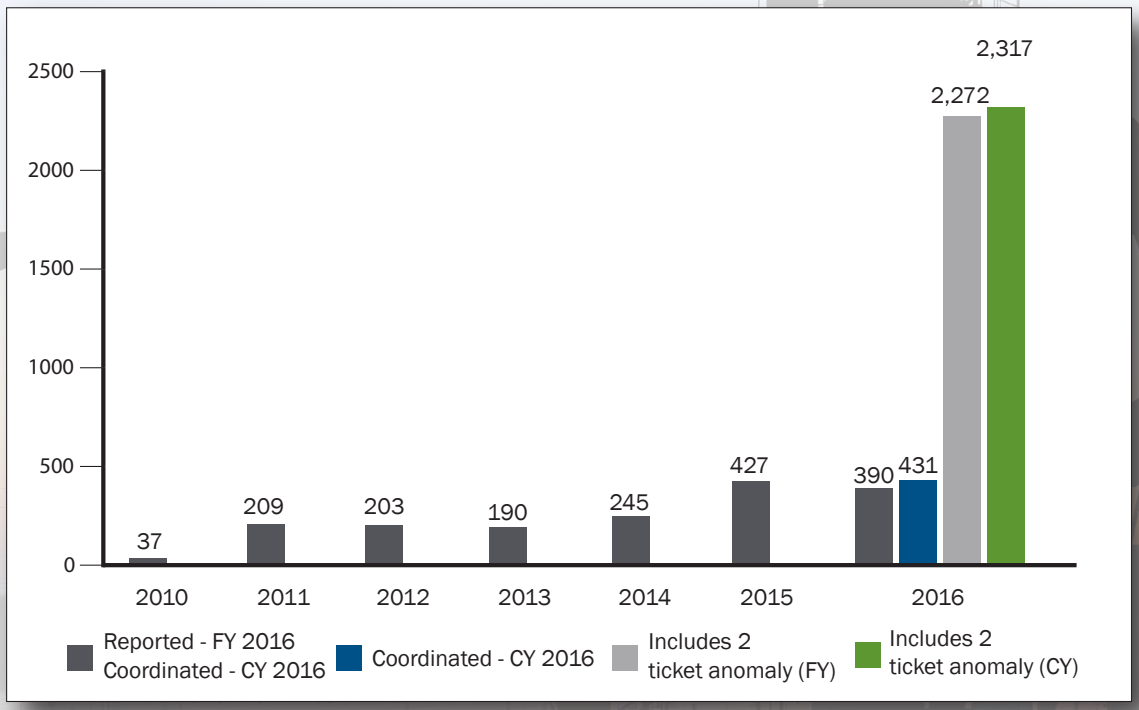

Figure 3. Vulnerabilities reported to ICS-CERT since FY 2010.

To help provide more granularity to the FY and CY 2016 data, Table 3 breaks down the total number of vulnerabilities coordinated. Out of the 2,282 reported vulnerabilities that ICS-CERT coordinated in FY 2016, the responsible product vendors refuted 10 vulnerabilities, resulting in 2,272 validated vulnerabilities. Excluding the 10 refuted vulnerabilities and the 1,878 outlier vulnerabilities, ICS-CERT performed data analysis on 394 validated vulnerabilities. Of these 394 validated vulnerabilities, ICS-CERT did not assign a Common Vulnerability Scoring System (CVSS) score to four vulnerabilities.

[2] The increase is primarily associated with two (2) tickets closed in 2016 that contain 1,418 and 460 vulnerabilities. Because these 1,878 validated vulnerabilities were associated with a small subset of affected products, there is some concern that these outliers could bias the metrics associated with vulnerability type and Common Vulnerability Scoring System (CVSS) scores. As a result, these are included in the total number of vulnerabilities reported to ICS-CERT; however, this data is not included in other metrics treated throughout this document.

In CY 2016, ICS-CERT received reports of 2,328 vulnerabilities. Of these, vendors refuted 11, resulting in 2,317 validated vulnerabilities. Excluding the 11 refuted vulnerabilities and the 1,878 outlier vulnerabilities previously mentioned, ICS-CERT performed data analysis on 439 vulnerabilities. ICS-CERT did not assign CVSS scores to eight of these 439 validated vulnerabilities. All vulnerability data for 2016 derives from vulnerabilities associated with vulnerability tickets closed during the specified reporting period. Table 3 provides a breakdown of vulnerabilities coordinated by ICS-CERT in 2016.

Year	Reported	Refuted	Total Validated	Excluded from Further Data Analysis 2	Validated Vulnerabilities	Validated Vulnerabilities with CVSS scores
FY 2016	2,282	10	2,272	1,878	394	390
CY 2016	2,328	11	2,317	1,878	439	431

Table 3. Vulnerabilities reported, validated and coordinated in FY and CY 2016.

Figure 4 details the percentage of coordinated vulnerabilities out of all validated vulnerabilities (coordinated and uncoordinated vulnerabilities) for FY and CY 2016 and for FY for prior years. The graphic does not include calendar year data for years prior to 2016. Due to the metrics reporting change in 2016, ICS-CERT advises caution when comparing data from FY 2016 with data from prior years.

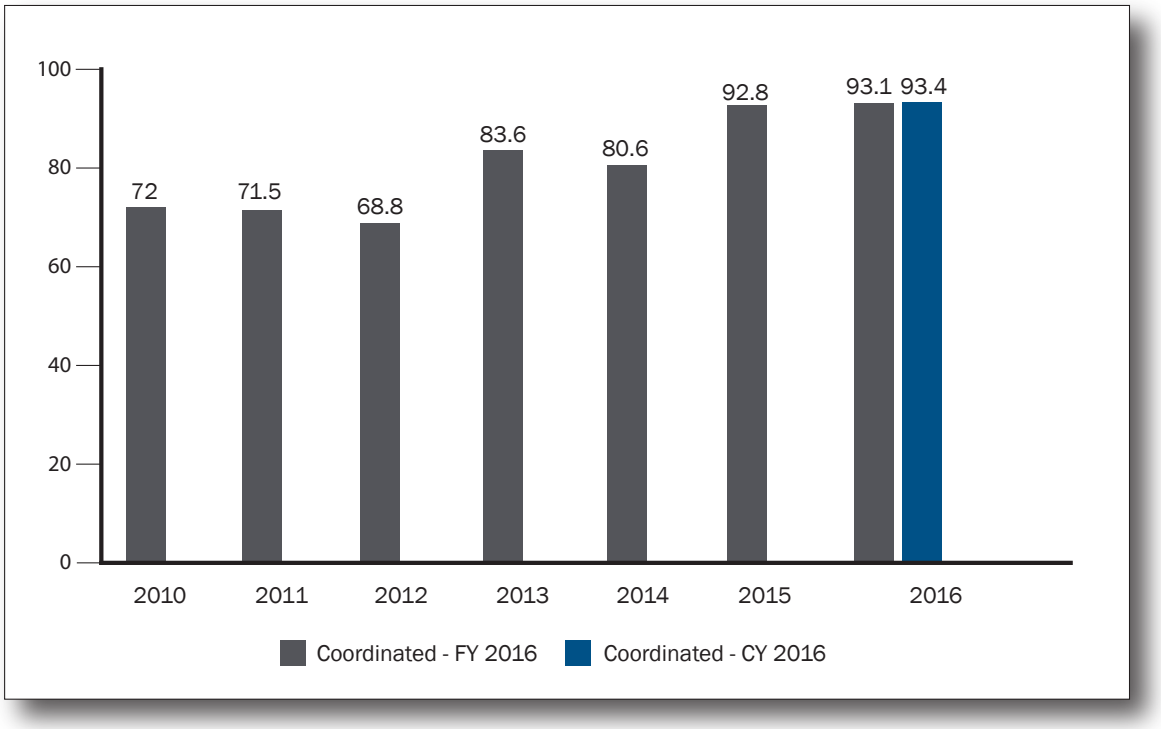

Figure 4. Percentage of coordinated disclosures since FY 2010 (FY and CY 2016 based on closed tickets).

7. VULNERABILITY TYPES AND SCORING

ICS-CERT categorizes and assesses the impact of validated vulnerabilities by assigning Common Weakness Enumeration (CWE) numbers and CVSS scores. In the following subsections, we provide the metrics associated with CWE and CVSS score assignments for validated vulnerabilities closed in CY and FY 2016.

7.1 Vulnerability Types

In FY 2016, ICS-CERT categorized and assigned 70 CWE numbers to 394 validated vulnerabilities. The four most frequently occurring CWEs were CWE-121: Stack-based Buffer Overflow; CWE-20: Improper Input Validation; CWE-79: Cross-site Scripting; and CWE-122: Heap-based Buffer Overflow.

In CY 2016, ICS-CERT categorized and assigned 85 CWE numbers to 439 validated vulnerabilities. The four most frequently occurring CWEs were CWE-121: Stack-based Buffer Overflow; CWE-122: Heap-based Buffer Overflow; CWE-20: Improper Input Validation; and CWE-79: Cross-site Scripting.

Figure 5 shows the most frequently assigned CWEs in FY and CY 2016 Each series shows the most frequent CWE assignments for 70 percent of all validated vulnerabilities during that reporting period.

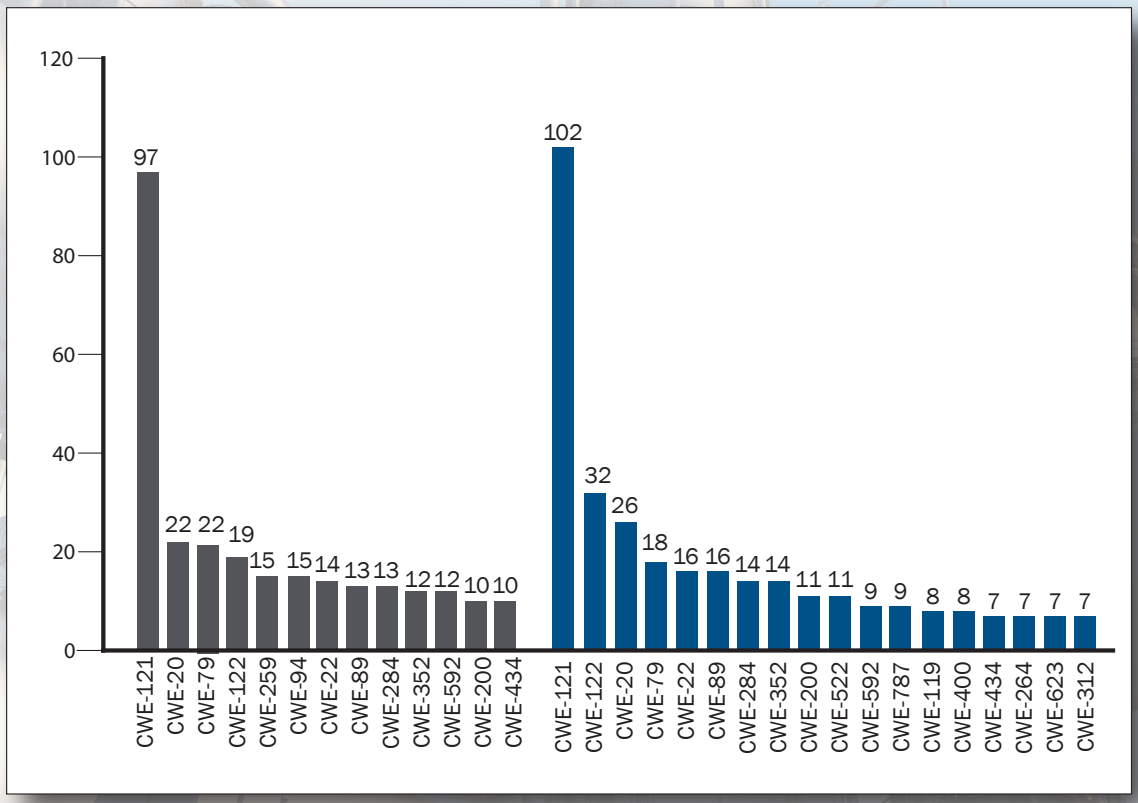

Figure 5. Most frequently assigned CWEs assigned by ICS-CERT in FY and CY 2016.

7.2 Vulnerability Impact Scoring

In FY 2016, ICS-CERT assigned CVSS scores to 390 validated vulnerabilities. In CY 2016, ICS-CERT assigned CVSS scores to 431 validated vulnerabilities. The average CVSS score for the vulnerabilities assessed by ICS-CERT was 7.8 out of 10. In FY and CY 2016, 71 and 73.8 percent of the vulnerabilities, respectively, have CVSS scores of seven and above. A CVSS score of seven or above indicates that these vulnerabilities, if exploited, have the potential to have a high or critical impact. Table 4 shows the distribution of the CVSS scores and general statistics about the scoring.

Year	Total Vulnerabilities Assigned CVSS	Score 9.0–10.0 (Critical)	Score 7–8.9 (High)	Score 4–6.9 (Medium)	Score 0 3.9 (Low)	CVSS Statistics (Average, Median, Hi-Low)
FY 16	390	158	119	104	9	Average: 7.8 Median: 7.5 Maximum: 10.0 Minimum: 2.2
CY 16	431	155	163	102	11	Average: 7.8 Median: 7.5 Maximum: 10.0 Minimum: 2.3

Table 4. CVSS scores and statistics for FY and CY 2016.

One of the more significant parameters associated with CVSS scores is Attack Vector, based on accessibility. This parameter gives some indication of the degree to which a vulnerability is exploitable. Of the 390 vulnerabilities assigned a CVSS score in FY 2016, 356 (91 percent) have an access vector of "Remote."

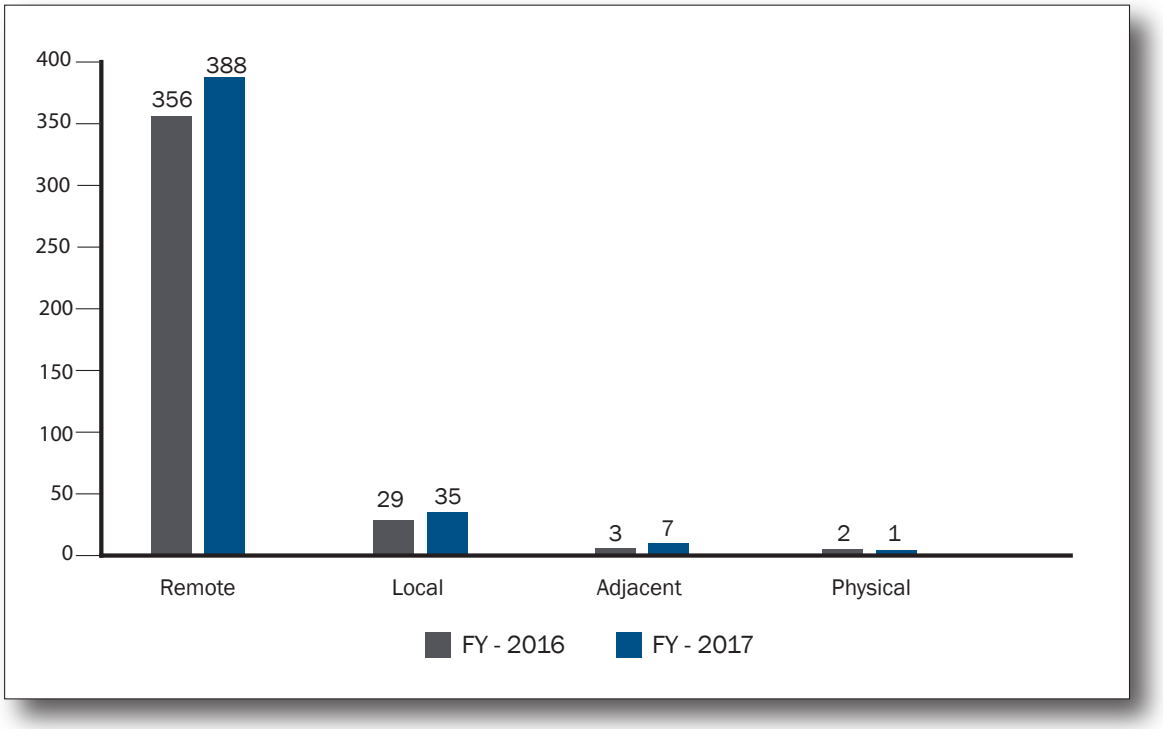

Figure 6. Access Vector data for the validated vulnerabilities with CVSS scores in FY and CY 2016.

7.3 Days to Close Vulnerability Tickets

In an attempt to provide greater visibility into ICS-CERT's vulnerability coordination process, we provide the information below regarding the time required to close a vulnerability ticket. Table 5 shows the ticket duration and closure rate information for FY and CY 2016.

Year	Number of Tickets Closed	Average Days to Close	Median Days to Close	Maximum Days to Close	Minimum Days to Close
FY16	143	128	94	680	2
CY16	162	135	98	901	2

Table 5. Ticket closure times for FY 2016.

8. VULNERABILITY RESOLUTION

ICS-CERT typically recommends that vendors produce product fixes for identified vulnerabilities. However, in some cases, it may not be possible for a vendor to offer a fix for unsupported products. In these situations, ICS-CERT works with the vendor to identify compensating controls to limit the risk of exploitation of an identified vulnerability.

Many of the researchers that ICS-CERT works with use tools and techniques that are not readily available to some vendors. Therefore, during the vulnerability coordination process, ICS-CERT recommends that vendors provide copies of their product fixes to the researchers who identified the associated vulnerabilities so they can validate the fix by using the same technique(s) they used to find the vulnerability originally.

In an attempt to capture vendor responsiveness to addressing reported vulnerabilities, ICS-CERT details the number of vulnerabilities for which product vendors have provided product fixes, as well as the number of researcher-validated fixes. Table 6 provides the FY an CY 2016 data for closed tickets.

Year	Validated Vulnerabilities	Fixes Provided by Product Vendors	Fixes Researchers Validated	Fixes Without Validation	Fixes Not Provided
FY16	394	363	54	309	31
CY16	439	392	55	337	47

Table 6. ICS vulnerability mitigation data for FY and CY 2016.

9. VULNERABILITY REPORTING TRENDS

In 2016, ICS-CERT received vulnerabilities from security researchers and product vendors. ICS-CERT observed an increase in the number of product vendors self-reporting vulnerabilities, which is a strong indicator of a mature or maturing security culture within an organization. To better understand and track this trend, ICS-CERT has broken down all of the validated vulnerabilities by reporting source for FY and CY 2016 in Table 7. Table 8 shows the researchers/non-vendor organizations and vendors who reported vulnerabilities for FY and CY 2016.

Year	Vulnerabilities	Vulnerabilities Reported by Researchers	Vulnerabilities Reported by Vendors
FY16	2,282	2,249 (98.6%)	33 (1.4%)
CY16	2,328	2,276 (97.8%)	52 (2.2%)

Table 7. Total vulnerabilities reported by vendors and researchers for FY and CY 2016.

Researchers and non-vendor organizations reporting FY and CY 2016		Vendors self-reporting FY and CY 2016
Ahmadi, Mike	Rios, Billy	ABB
Beyah, Raheem	Rupp, Maxim	Emerson
Caltabiano, Ariele (kimiya)	Sanchez, Ivan	GE
Dashchenko, Vladimir	Sands, Fritz	Honeywell
Ganeshen, Karn	Seeley, Steven	OSISoft
Giller, Nir	Smith, Neil	Rockwell Automation
Gritsai, Gleb	Sood, Aditya	Schneider Electric
Karpov, Ilya	Temnikov, Sergey	Siemens
Lo, Andrew (Yun Ting)	Yu, Zhou	Smiths-Medical
Micalizzi, Andrea (rgod)	Zero Day Initiative (ZDI)	Yokogawa

Table 8. Researchers/non-vendor organizations and vendors who reported vulnerabilities for FY and CY 2016.

10. SECTOR DATA

Figure 7 shows the vulnerabilities coordinated by ICS-CERT in FY and CY 2016 by CI sector in which the product is used.

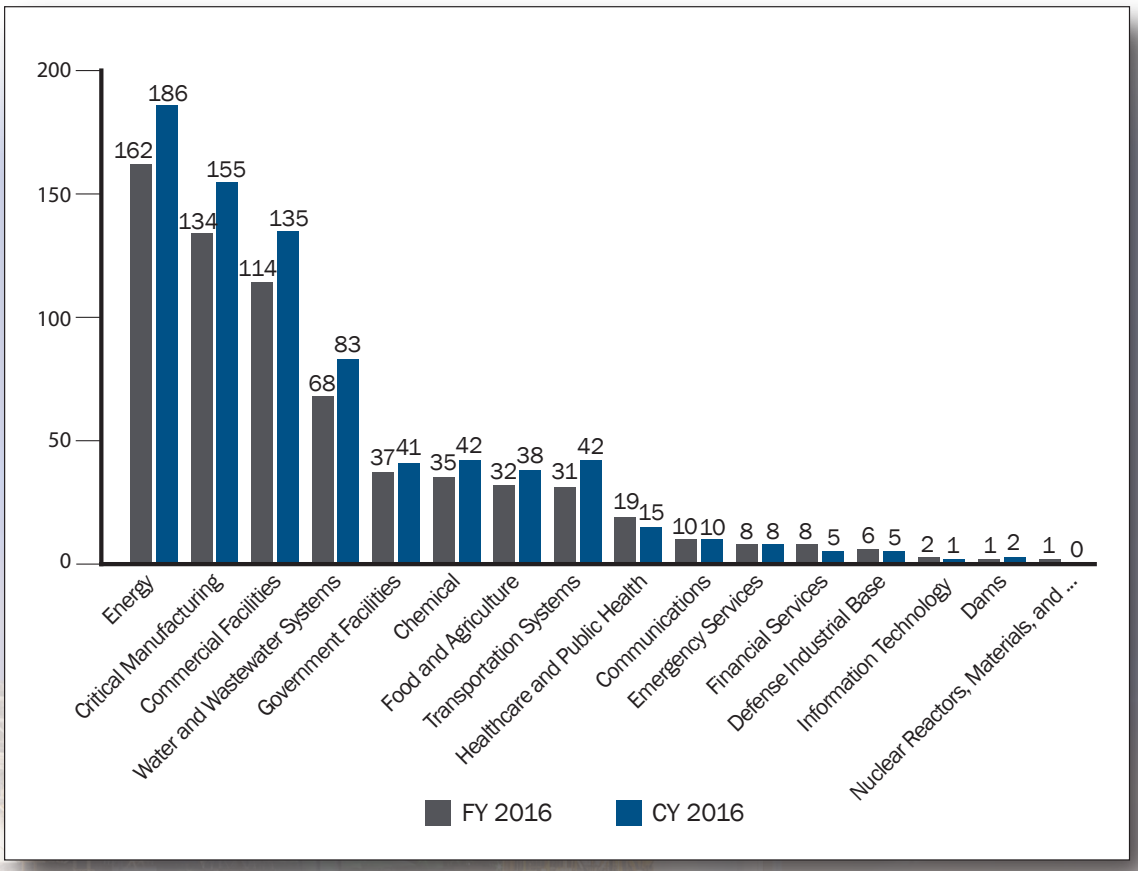

Figure 7. Coordinated vulnerabilities by critical infrastructure sector for FY and CY 2016.

11. SUMMARY

In FY and CY 2016, ICS-CERT released 157 and 185 advisories, respectively, and 17 alerts during both reporting periods. The number of vulnerabilities reported to ICS-CERT in FY and CY 2016 were 2,282 and 2,328 vulnerabilities, respectively. The Vulnerability team performed a more detailed analysis on a subset of the reported vulnerabilities. Cybersecurity researchers reported 98.6 percent of the vulnerabilities reported to ICS-CERT and product vendors self-reported the remaining 1.4 percent. The most frequently occurring vulnerability types encountered by ICS-CERT were Stack-based Buffer Overflow, Improper Input Validation, Cross-site Scripting, and Heap-based Buffer Overflow vulnerabilities. The average CVSS score for the vulnerabilities assessed by ICS-CERT was 7.8 out of 10. In FY and CY 2016, 71 and 73.8 percent of the vulnerabilities, respectively, have CVSS scores of seven and above. A CVSS score of seven or above indicates that these vulnerabilities, if exploited, have the potential to have a high or critical impact.

In FY and CY 2016, ICS-CERT coordinated product vulnerabilities with product vendors that provided product fixes for 363 and 392 vulnerabilities, respectively, which correspond to product fixes for 92.1 percent and 89.3 percent of the vulnerabilities reported to ICS-CERT. The majority of the vulnerabilities coordinated by ICS-CERT in 2016 were most commonly associated with the Energy, Critical Manufacturing, Commercial Facilities, Water and Wastewater Systems Sectors.

Contact ICS-CERT

ICS-CERT encourages you to report suspicious cyber activity and vulnerabilities affecting critical infrastructure control systems.

U.S. Toll Free: 1-877-776-7585

International: (208) 526-0900

Email: ics-cert@hq.dhs.gov

Web site: https://ics-cert.us-cert.gov

ICS-CERT Report an Incident page: https://ics-cert.us-cert.gov/Report-Incident?

ICS-CERT Information page: https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

Contact NCCIC

NCCIC encourages you to report suspicious cyber activity and vulnerabilities affecting government or critical infrastructure enterprise IT systems.

NCCIC Service Desk and Customer Service

Phone: (888) 282-0870

Email: NCCICCustomerService@hq.dhs.gov

To speak with or to contact the NCCIC Duty officer (24x7)

Phone: (703) 235-5273

Email: NCCIC@hq.dhs.gov

NCCIC