ToolsWatch.Org
November 5, 2015

ICS/SCADA Top 10 Most Dangerous *Software* Weaknesses

by NJ OUCHN

This study is not affiliated with the MITRE Corporation even if the title has a similarity in its formulation with the **CWE/SANS Top 25 Most Dangerous Software Errors**[1]. In fact, it is my own initiative led in the context of statistics validation regarding the vulnerability databases.

[1] http://cwe.mitre.org/top25/

Technological progress is like an axe in the hands of a pathological criminal.

-Albert Einstein

The followed methodology is quite different from the MITRE since it is based on statistical data extracted from vFeed[2] the Vulnerability and threat Database. The MITRE methodology leveraged the Common Weakness Scoring System[3] (CWSS) to categorize and assess the weaknesses scores by over 20 contributing organizations.

Therefore, I have found it useful to focus on the vulnerabilities and weaknesses related to the Industrial Systems as they are increasingly targeted by new sophisticated attacks.

According to the SANS security experts, during the previous RSA conference, the Industrial System Controls attacks were listed amongst the top 6 emerging and trending new techniques.

[2] https://github.com/toolswatch/vFeed

[3] http://cwe.mitre.org/cwss

The **ICS/SCADA Top 10 Most Dangerous Software Weaknesses** list has been compiled on the basis of the following assumptions :

1. The vulnerability database used in this research is vFeed (Database build 10032015). The latter was developed with the main objective to collect and correlate a maximum of information issued by third party vendors. The database accuracy and coverage were thoroughly validated by the MITRE.
   vFeed has been awarded with 3 certifications[4] : Common Vulnerability Enumeration (CVE), Common Weakness Enumeration (CWE) and Open Vulnerability Assessment Language (OVAL) . A piece of code which relied on to collect and analyze the big amount of information is provided in the Appendix.

2. The analyzed vulnerabilities are fundamentally associated with the manufacturers listed by the ISC-CERT. This approach seemed to be rational since the ISC-CERT[5] officially coordinates the disclosure of security threats and vulnerabilities regarding the Industrial Control Systems. *The list of vendors is provided in the Appendix*.

3. Numerous vulnerabilities are missing the CWE identifier. As a matter of fact the National Vulnerability Database[6] (NVD) only supports the CWEs listed here https://nvd.nist.gov/cwe.cfm#cwes
   Currently and in the context of this study, I have identified 147 CVEs related to 469 different products missing a CWE. However it was fairly simple to identify the missing adequate CWE. Nevertheless,it is time consuming and not the purpose of this paper. I will later communicate the list to NVD with a proposal of the missing CWEs.

4. Each CPE is treated as unique. Therefore, a vendor whose product containing several vulnerable versions (CPEs) to the same CVE will be counted as many.
   Ex: CVE-2012-4690 (CWE-16) hits 4 separate versions of the product *Micrologix Controller* edited by *Rockell Automation.* Therefore, the CWE-16 is counted 4 times. Which is perfectly logical in my opinion.

5. The most vulnerable products are the most known and widely used by the industries. Therefore when a vendor wins a worldwide reputation, he must acknowledge it.

6. The Excel spreadsheet used for this paper can be obtained freely by email request to hacker@toolswatch.org or via twitter (@toolswatch)

---

[4] https://github.com/toolswatch/vFeed/wiki/%5B1%5D-vFeed-Framework-(API-&-Correlated-Vulnerability-Database)

[5] https://ics-cert.us-cert.gov/alerts-by-vendor

[6] https://nvd.nist.gov/

The ICS/SCADA Top 10 List

Rank	ID	Title
1	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
2	CWE-20	Improper Input Validation
3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
4	CWE-264	Permissions, Privileges, and Access Controls
5	CWE-200	Information Exposure
6	CWE-255	Credentials Management
7	CWE-287	Improper Authentication
8	CWE-399	Resource Management Errors
9	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
10	CWE-189	Numeric Errors

CWE-119
The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.

CWE-20
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 will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution

CWE-22
The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

CWE-264
Weaknesses in this category are related to the management of permissions, privileges, and other security features that are used to perform access control.ry.

CWE-200
An information exposure is the intentional or unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information.

CWE-255
Weaknesses in this category are related to the management of credentials.

CWE-287
When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.

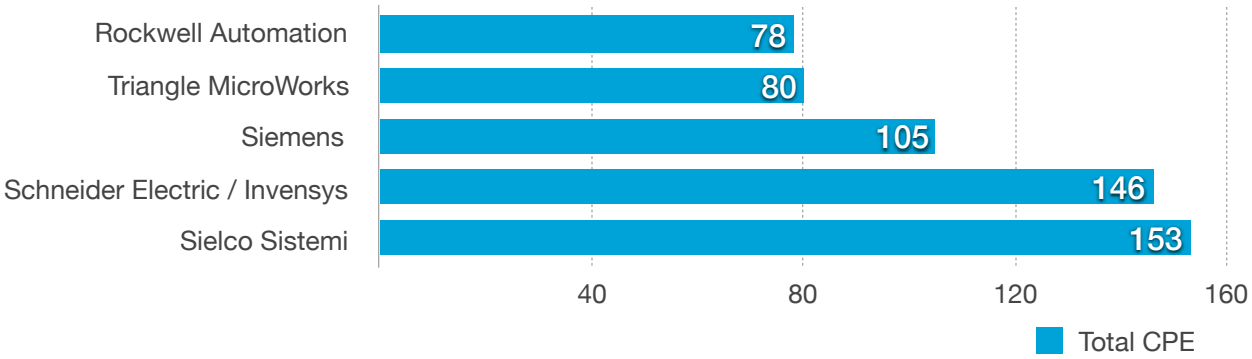
CWE-399
Weaknesses in this category are related to improper management of system resources.

CWE-79
The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

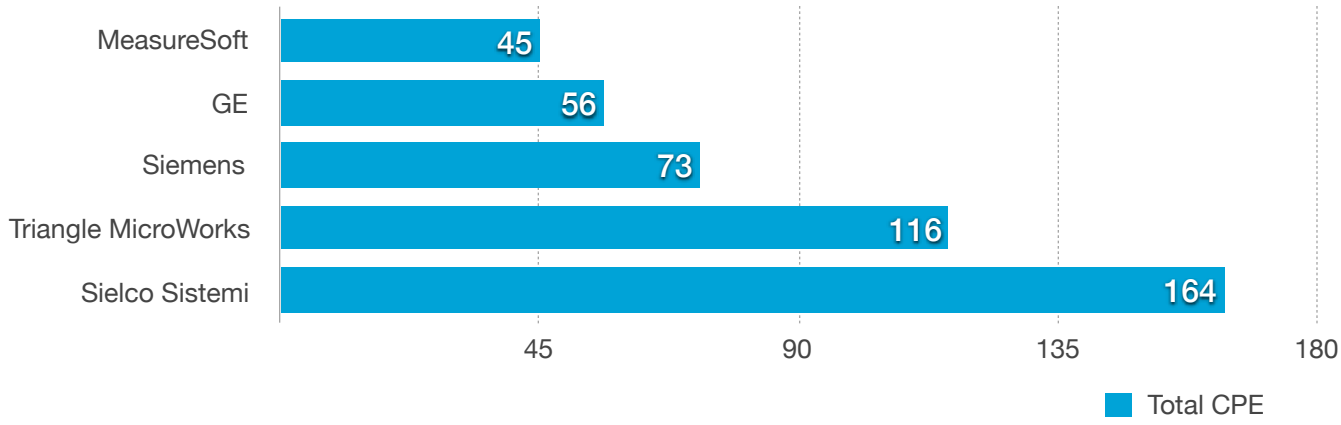
CWE-189
Weaknesses in this category are related to improper calculation or conversion of numbers.

Affected Vendors per Category of Weaknesses

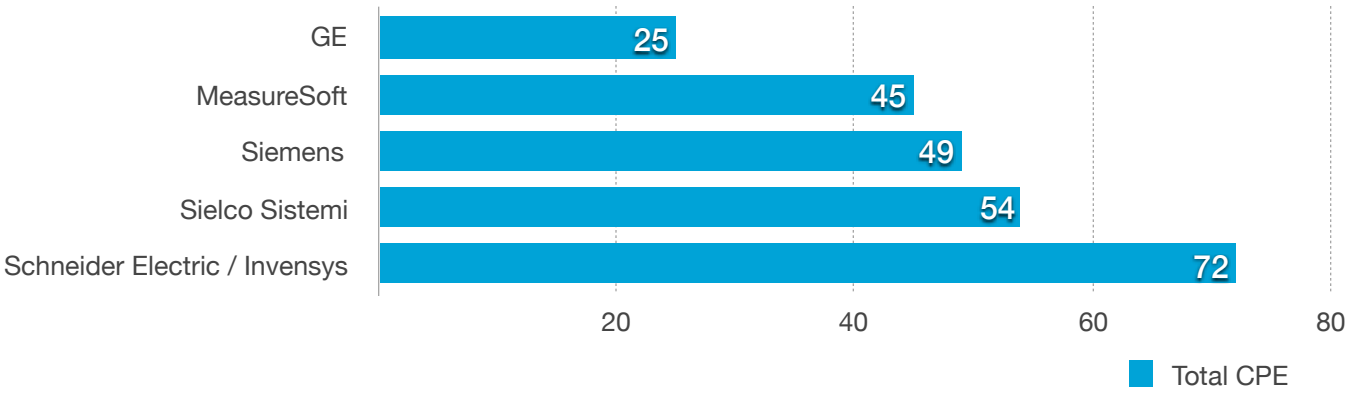
CWE-119 Top 5 affected Vendors



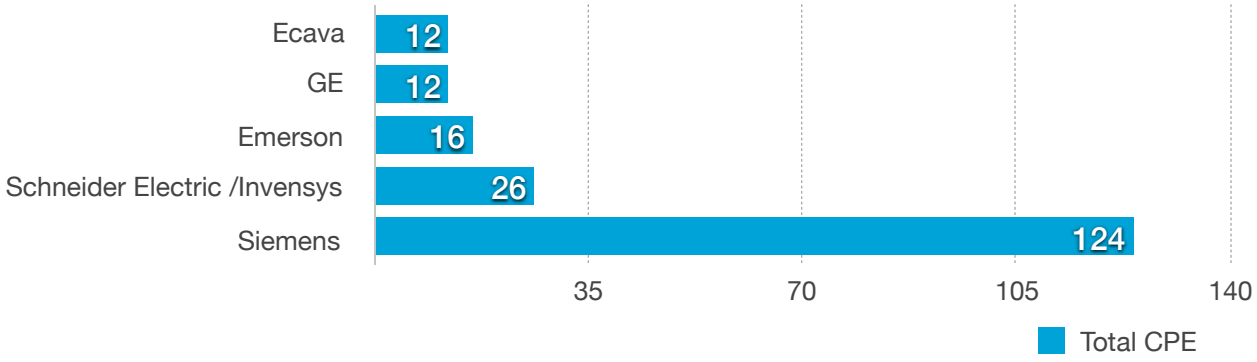
CWE-20 Top 5 affected Vendors



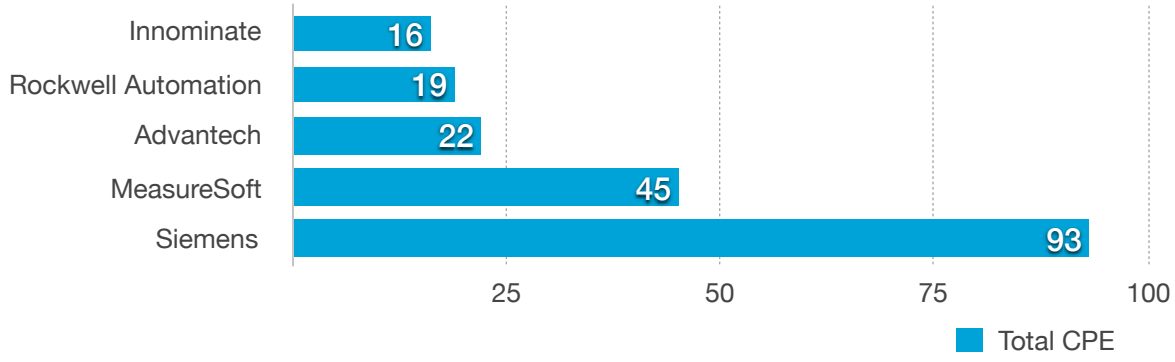
CWE-22 Top 5 affected Vendors



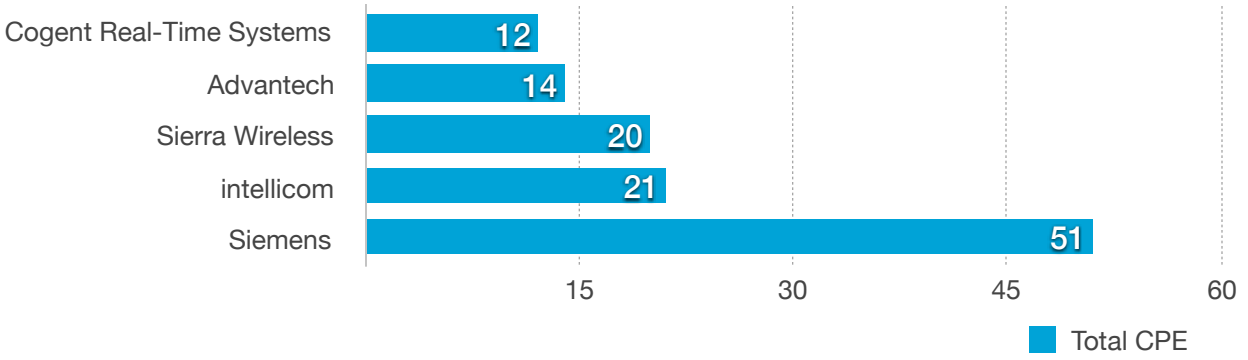
CWE-264 Top 5 affected Vendors



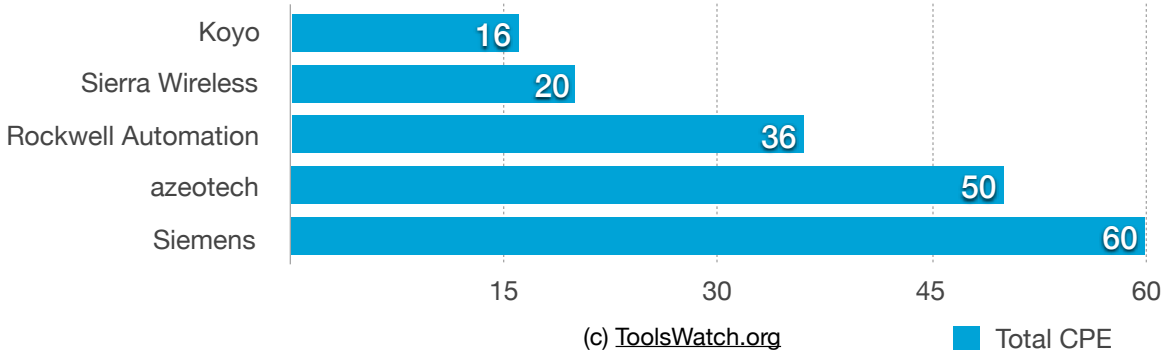
CWE-200 Top 5 affected Vendors

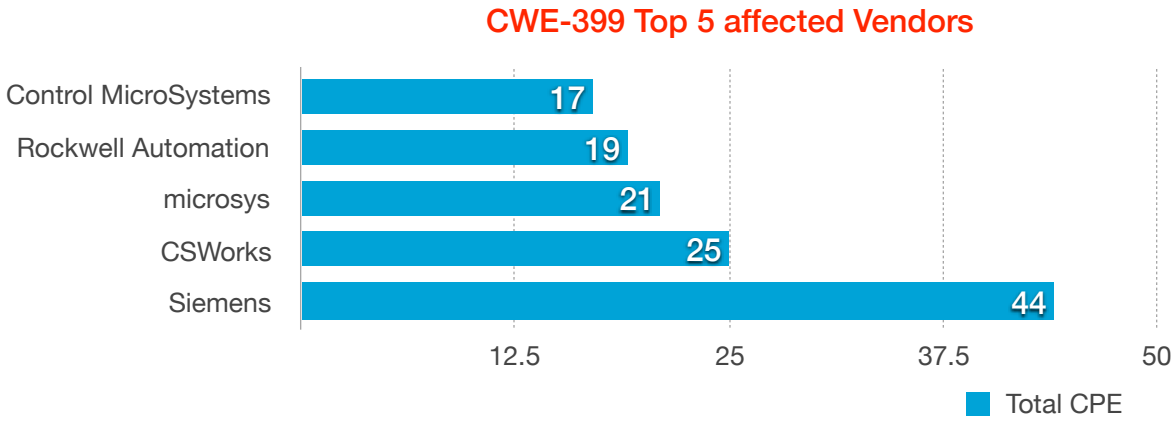


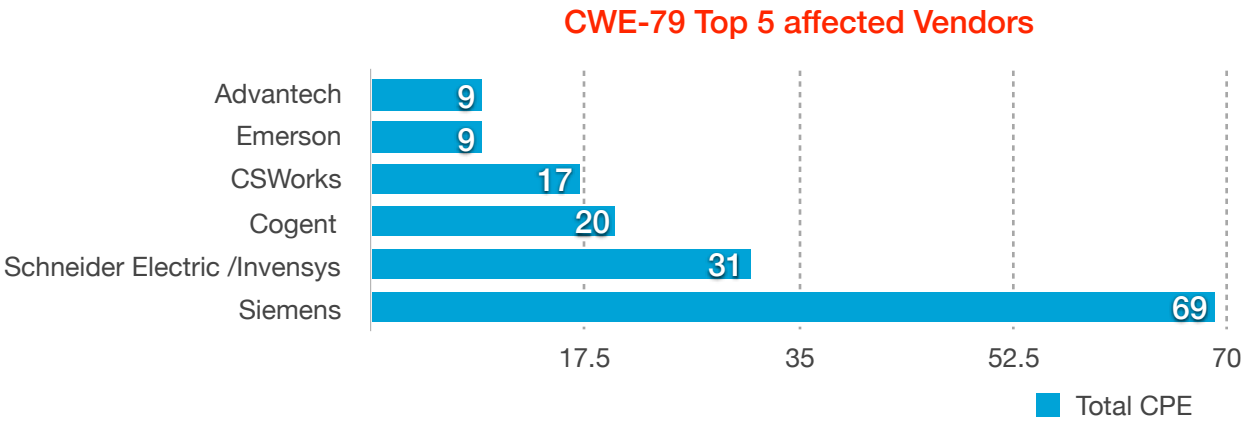
CWE-255 Top 5 affected Vendors

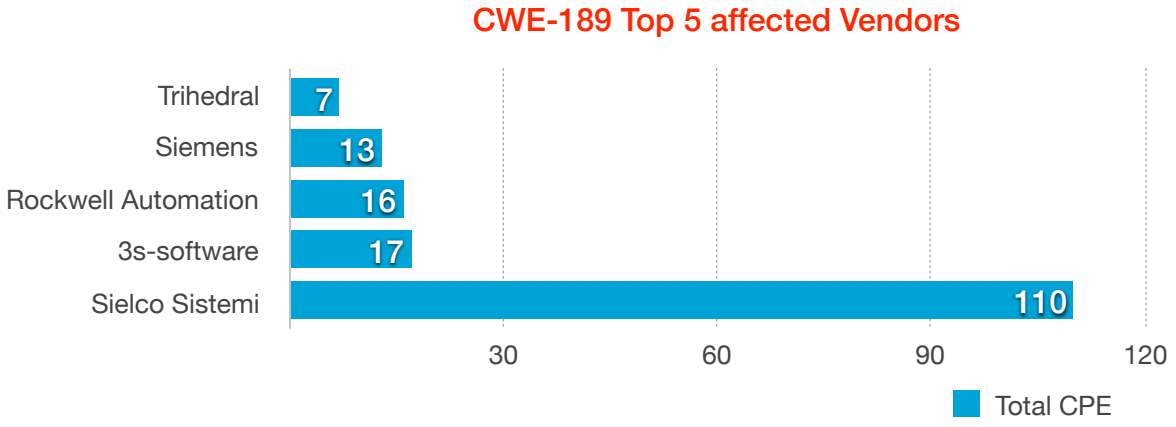


CWE-287 Top 5 affected Vendors




CWE-399 Top 5 affected Vendors
Control MicroSystems
Rockwell Automation
microsys
CSWorks
Siemens
17
19
21
25
44
12.5
25
37.5
50
Total CPE


CWE-79 Top 5 affected Vendors
Advantech
Emerson
CSWorks
Cogent
Schneider Electric /Invensys
Siemens
9
9
17
20
31
69
17.5
35
52.5
70
Total CPE


CWE-189 Top 5 affected Vendors
Trihedral
Siemens
Rockwell Automation
3s-software
Sielco Sistemi
7
13
16
17
110
30
60
90
120
Total CPE

Appendix

360 Systems
3S-Smart Software Solutions
7-Technologies
ABB
Accuenergy
Advantech
Alstom
Amtelco
Arbiter Systems
ARC Informatique
Areva
Automated Solutions
AzeoTech
Atvise
Beckhoff
Beijer Electronics
C3-ilex
Canary Labs, Inc.
CareFusion
Carlo Gavazzi
Catapult Software
Certec
Citect
Clorius Controls
CG Automation
Cisco
Cogent Real-Time Systems Inc
Cobham
Cooper Power Systems
Copa-Data
Control MicroSystems
CSWorks
Digi International
Digital Electronics
Ecava
Elecsys

Elipse
Emerson
Fanuc
Festo
Fox-IT
Fultek
Galil
GarrettCom
GE
LiveData
Gesytec
Honeywell
I-GEN
Iconics
Inductive Automation
InduSoft
Innominate
Intellicom
IOServer
Kepware Technologies
Korenix
Koyo
MatrikonOPC
MeasureSoft
Meinberg
Microsys
Mitsubishi Electric Automation
Monroe Electronics
Morpho
Moxa
National Instruments
NETxAutomation
Nordex
NovaTech
Ocean Data
OleumTech
Omron
Open Automation Software

Optimalog
ORing
OSIsoft
Philips
Phoenix Contact Software
Post Oak Traffic Systems
Progea
ProSoft Technology
QNX
RealFlex Technologies
Rockwell Automation
RuggedCom
SafeNet
Samsung
SCADA Engine
ScadaTEC
Schneider Electric
Schweitzer Engineering Laboratories
Sensys Networks
Sielco Sistemi
Siemens
Sierra Wireless
Sinapsi
Sixnet
Sisco
Software Toolbox
SpecView
Subnet Solutions Inc.
Sunway
Takebishi Electric
Triangle MicroWorks
Tridium
Trihedral Engineering Ltd
Tropos
Turck
Unitronics
Wago
WellinTech

Wind River Systems

xArrow

Xzeres

Yokogawa

Code used to extract data

```
#!/usr/bin/env python

from lib.core.search import Search

def check_app(product_app):
    try:
        Search(product_app)
    except:
        return

def check_os(product_os):
    try:
        Search(product_os)
    except:
        return

def check_hw(product_hw):
    try:
        Search(product_hw)
    except:
        return

def main():
    print '================================================================='
    print "ICS/SCADA Top 10 Most Dangerous Software Errors "
    print '================================================================='

    vendor_list = 'vendors.txt'
    vendor_list = open(vendor_list, "r")
    for line in iter(vendor_list):
        line = line.strip().split(";")
        #print "vendor:", line[0]
        products = line[1].strip().split(",")
        for product in products:
            product_app = product
            check_app(product_app)
            product_os = product.replace("cpe:/a:","cpe:/o:")
            check_os(product_os)
            product_hw = product.replace("cpe:/a:","cpe:/h:")
            check_hw(product_hw)

if __name__ == '__main__':
    main()
```