

# Securing ICS Applications When Vendors Refuse Or Are Slow To Produce a Security Patch





& Luigi Auriemma

[twitter.com/luigi\\_auriemma](https://twitter.com/luigi_auriemma)

& Donato Ferrante

[twitter.com/dntbug](https://twitter.com/dntbug)

# Who?

⌘ Vulnerability Feeds

⌘ 0-day

⌘ 1-day

⌘ SCADA defense

⌘ SCADA-shield

⌘ Penetration Testing

⌘ Consulting

# About ReVuln

[revuln.com](http://revuln.com)

[info@revuln.com](mailto:info@revuln.com)

[twitter.com/revuln](https://twitter.com/revuln)



& Security Vulnerabilities

& Uncovering new vulnerabilities

& Final considerations

# Agenda

4



ReVuln Ltd.

## & **Security Vulnerabilities**

- ⌘ Problems
- ⌘ Possible solutions
- ⌘ Some numbers

## & Uncovering new vulnerabilities

## & Final considerations

# Agenda




# Security Vulnerabilities

6



ReVuln Ltd.

- 
- A large, dark, billowing cloud of smoke and fire, resembling a nuclear explosion, dominates the right side of the slide. The fire is bright orange and yellow, contrasting sharply with the dark smoke and the dark blue background.
- ⌘ Downtime
  - ⌘ Information stealing
  - ⌘ Bridge-attack/**SmartGrid**
  - ⌘ Remote control/**pwn**

# Problems



# Possible Solutions

8



ReVuln Ltd.



## ⌘ Vendor Patches

- ⌘ Take time
- ⌘ **Reactive**
- ⌘ May **NOT** fix the security issue
- ⌘ NO information = NO patch

# Possible Solutions - I



## ⌘ Unofficial Patches

- ⌘ **Require knowledge** of the security issues
- ⌘ Sometimes it's not easy/quick to fix an issue
- ⌘ It may affect checksums
- ⌘ NO information = NO patch

# Possible Solutions - II



- ⌘ Signatures-based defenses (IPS/IDS)
  - ⌘ **Require knowledge** of the security issues
    - ⌘ NO information = NO signatures
  - ⌘ Work ONLY on few exploit “patterns”
    - ⌘ **Exploit mutation** usually breaks these detections

# Possible Solutions - III



## ⌘ SCADA shield

- ⌘ Pro-Active solution
- ⌘ Combine information from internal vulnerability feeds, and exploit prevention techniques to provide a shield to most of the pre-existent HMI/SCADA solutions

# Possible Solutions - IV



⌘ Tries to prevent **classes of vulnerabilities**, i.e.:

- ⌘ Directory traversal
- ⌘ File Inclusion/Overwriting
- ⌘ Stack and Heap Overflow
- ⌘ Use-After-Free
- ⌘ Commands Injection

⌘ DEMO'ed during S4 2013

# SCADA Shield - I



- ⌘ Allows to perform **Hot-Patching**
  - ⌘ **In-memory patch**
    - ⌘ No need to restart/interrupt the system
    - ⌘ Vendor's products warranty NOT voided

# SCADA Shield - II



⌘ We wanted more..

- ⌘ In the current release we are testing a **custom detection engine**
- ⌘ Our idea is to be able to integrate our feeds with SCADA shield signatures
- ⌘ Our SCADA customers will be able to import SCADA shield signatures **on-the-fly to protect their systems**

# SCADA Shield - III



# Some Numbers

16



ReVuln Ltd.



We consider only  
remote vulnerabilities..

Advisory Name:	Released:	Fixed*:
realwin_1	15 oct 2010	-> 08 nov 2010
inbatch_1	07 dec 2010	-> 02 mar 2011
integraxor_1	21 dec 2010	-> 12 jan 2011
winlog_1	12 jan 2011	-> 13 jan 2011
realwin_2/8	21 mar 2011	-> 20 apr 2011
igss_1/8	21 mar 2011	-> 06 may 2011*
genesis_1/13	21 mar 2011	-> 18 apr 2011
factorylink_1/6	21 mar 2011	-> 05 apr 2011
bwocxrun_1	02 sep 2011	-> 17 feb 2012
twincat_1	13 sep 2011	-> 06 oct 2011
scadapro_1	13 sep 2011	-> 20 sep 2011
rslogix_1	13 sep 2011	-> 06 oct 2011
movicon_*	13 sep 2011	-> 21 oct 2011
daqfactory_1	13 sep 2011	-> 21 sep 2011
pcvue_1	27 sep 2011	-> 06 dec 2011
opcnet_1	10 oct 2011	-> 25 jan 2012
webmi2ads_1	10 oct 2011	-> 17 jan 2012
		11 apr 2012
promotic_1	13 oct 2011	-> 23 jan 2012
promotic_2	30 oct 2011	-> 11 apr 2012
ifix_1	06 feb 2011	-> 07 nov 2011
optimalog_1	13 nov 2011	-> 27 sep 2012
winccflex_1	28 nov 2011	-> 18 apr 2012
indusoft_*	27 apr 2011	-> 16 nov 2011
almsrvx_1	28 nov 2011	-> 26 dec 2011*
codesys_1	29 nov 2011	-> 06 jan 2012
		14 nov 2012
kingview_1	09 nov 2011	-> 22 dec 2011
rnadiagreceiver_1	17 jan 2012	-> 06 apr 2012
abb_1	10 oct 2011	-> 22 feb 2012
xarrow_1	02 mar 2012	-> 24 may 2012
rtip_1	17 oct 2011	-> 22 aug 2012
ifix_2	17 oct 2011	-> 03 aug 2012
suitelink_1	11 may 2012	-> 19 jun 2012
proservrex_1	13 may 2012	-> 27 jun 2012
winlog_2	26 jun 2012	-> 31 jul 2012
specview_1	29 jun 2012	-> 12 jan 2012

Raw data..



We consider only  
remote vulnerabilities..

Tags..

18



ReVuln Ltd.

Advisory Name:	Released:	Fixed*:
realwin_1	15 oct 2010	-> 08 nov 2010
inbatch_1	07 dec 2010	-> 02 mar 2011
integraxor_1	21 dec 2010	-> 12 jan 2011
realwin_2/8	21 mar 2011	-> 20 apr 2011
igss_1/8	21 mar 2011	-> 06 may 2011*
genesis_1/13	21 mar 2011	-> 18 apr 2011
factorylink_1/6	21 mar 2011	-> 05 apr 2011
bwocxrun_1	02 sep 2011	-> 17 feb 2012
twincat_1	13 sep 2011	-> 06 oct 2011
scadapro_1	13 sep 2011	-> 20 sep 2011
rslogix_1	13 sep 2011	-> 06 oct 2011
movicon_*	13 sep 2011	-> 21 oct 2011
daqfactory_1	13 sep 2011	-> 21 sep 2011
pcvue_1	27 sep 2011	-> 06 dec 2011
opcnet_1	10 oct 2011	-> 25 jan 2012
webmi2ads_1	10 oct 2011	-> 17 jan 2012
		11 apr 2012
promotic_1	13 oct 2011	-> 23 jan 2012
promotic_2	30 oct 2011	-> 11 apr 2012
almsrvx_1	28 nov 2011	-> 26 dec 2011*
codesys_1	29 nov 2011	-> 06 jan 2012
		14 nov 2012
rnadiagreceiver_1	17 jan 2012	-> 06 apr 2012
xarrow_1	02 mar 2012	-> 24 may 2012
suitelink_1	11 may 2012	-> 19 jun 2012
proservrex_1	13 may 2012	-> 27 jun 2012
winlog_2	26 jun 2012	-> 31 jul 2012
specview_1	29 jun 2012	-> 12 jan 2012
winlog_1	12 jan 2011	-> 13 jan 2011
ifix_1	06 feb 2011	-> 07 nov 2011
indusoft_*	27 apr 2011	-> 16 nov 2011
kingview_1	09 nov 2011	-> 22 dec 2011
abb_1	10 oct 2011	-> 22 feb 2012
rtip_1	17 oct 2011	-> 22 aug 2012
ifix_2	17 oct 2011	-> 03 aug 2012

Not Reported

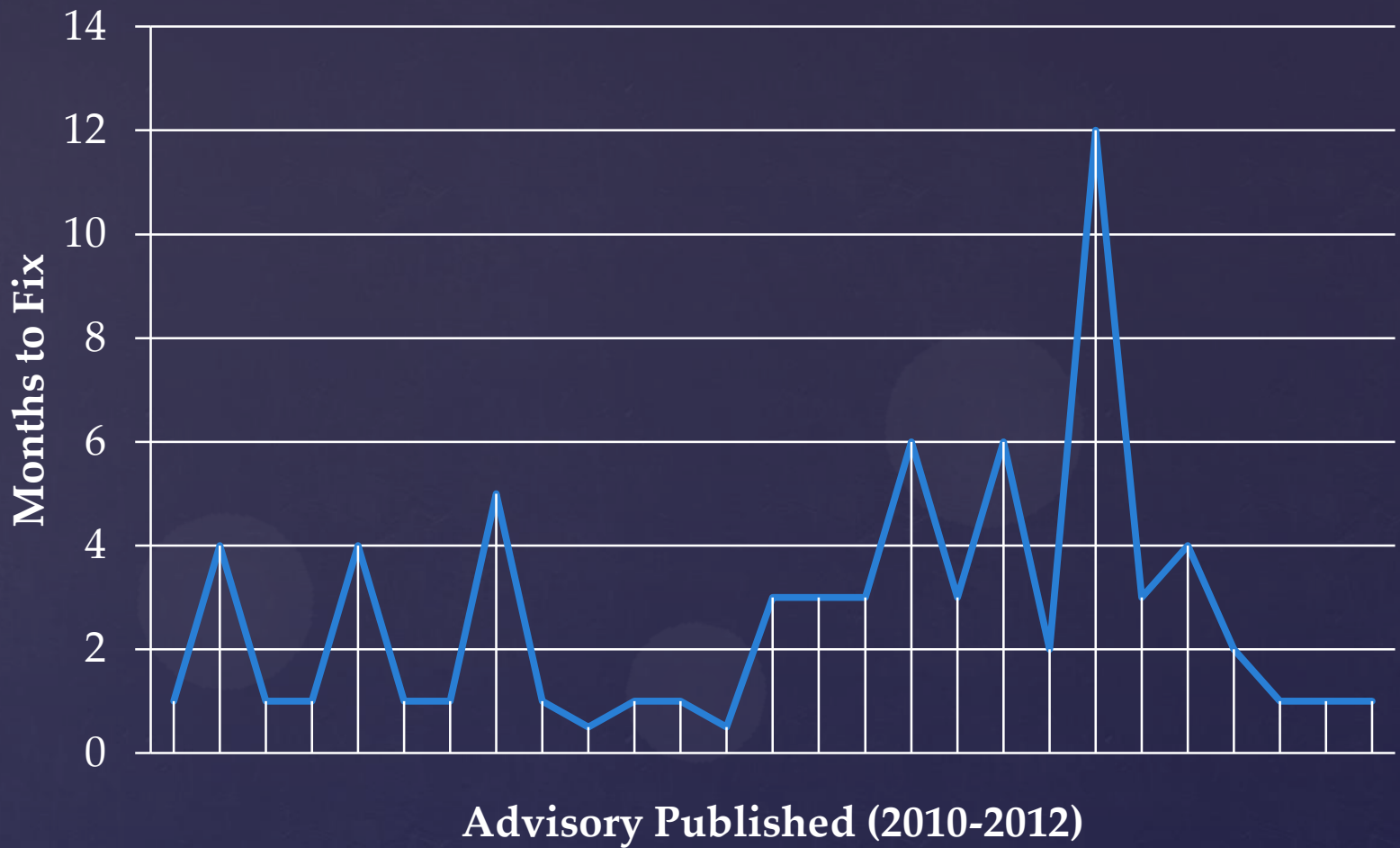
Reported

Advisory Name:	Released:	Fixed*:
winlog_1	12 jan 2011 ->	13 jan 2011 +0
kingview_1	09 nov 2011 ->	22 dec 2011 +1
abb_1	10 oct 2011 ->	22 feb 2012 +4
indusoft_*	27 apr 2011 ->	16 nov 2011 +7
ifix_1	06 feb 2011 ->	07 nov 2011 +9
rtip_1	17 oct 2011 ->	22 aug 2012 +10
ifix_2	17 oct 2011 ->	03 aug 2012 +10

> 3 month

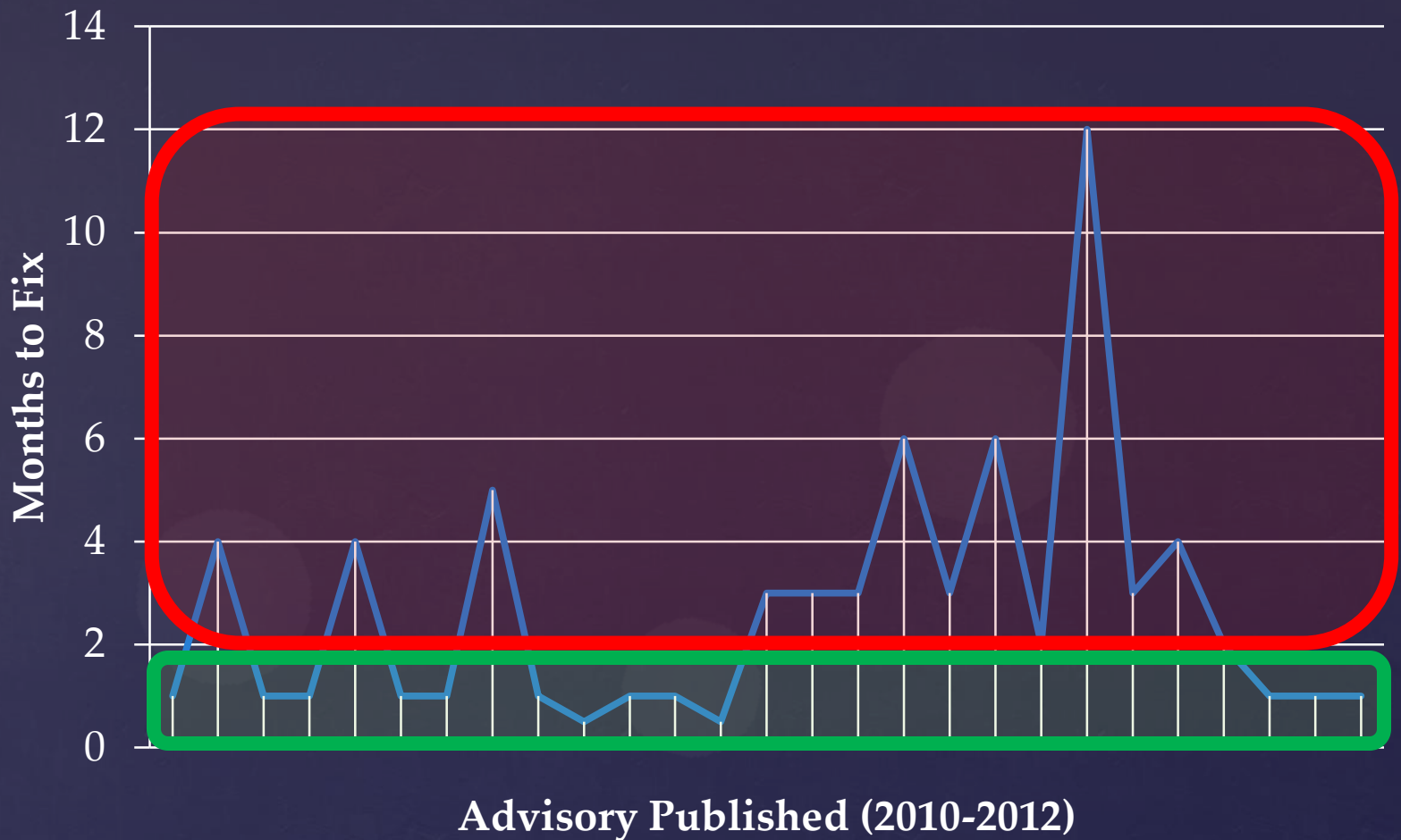
# Reporting issues to Vendors doesn't speed up fixing..





# When Vendors fix the issues..





# When Vendors fix the issues..



### Advisory (ICSA-12-271-02)

#### Optimalog Optima PLC Multiple Vulnerabilities

Original release date: September 27, 2012 | Last revised: April 22, 2013

<http://ics-cert.us-cert.gov/advisories/ICSA-12-271-02>

Optimalog's recommendation to all users that plan to use APIFTP Server is to configure their firewall and VPN accordingly and set the program to run at startup of the station. If a user does not plan to use APIFTP server, then disable its execution.

Fixed? No. But the users will get a  
**RECOMMENDATION** instead...

Advisory Name:	Released:	Fixed*:
optimalog_1	13 nov 2011	-> 27 sep 2012
winccflex_1	28 nov 2011	-> 18 apr 2012

# And when they don't..





## & Security Vulnerabilities

- ⌘ Problems
- ⌘ Possible solutions
- ⌘ Some numbers

## & Uncovering new vulnerabilities

## & Final considerations

# Agenda





# Uncovering new vulnerabilities

24



ReVuln Ltd.



- & General Electric
- & Siemens
- & ABB
- & Rockwell
- & Invensys
- & Schneider
- & InduSoft
- & CoDeSys
- & ...

# Vendors



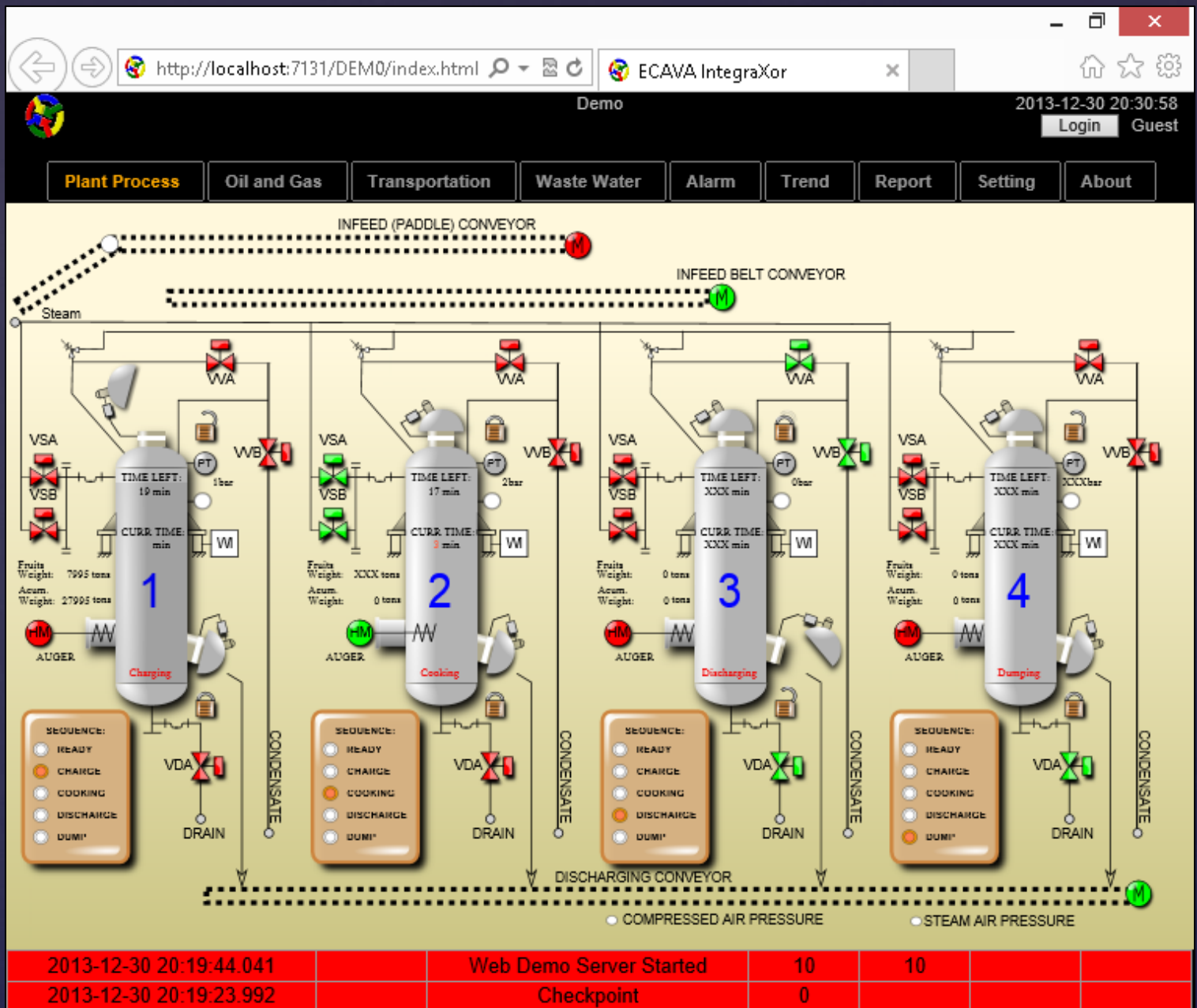
## Product: **IntegraXor**

- ⌘ <http://www.integraxor.com>
- ⌘ Tested **versions <= 4.1.4380**
- ⌘ Default port: 7131 TCP
- ⌘ Protocol: HTTP
- ⌘ Status: **0-day**

IntegraXor SCADA is a pure **Webserver** that developed based on W3C standard compliant technologies. No additional web server is needed so installation is very simple and yet cost effective. This also means no additional client program nor plug-in needed except a modern browser for viewing/accessing the mimic screen. So this is a Browser/ Server system rather than ordinary Client/Server system.

# The Product






27



ReVuln Ltd.

# The Web interface



**SCADA VENDOR OFFERS STORE CREDIT FOR VULNERABILITIES**

by **Brian Donohue** [Follow @TheBrianDonohue](#) July 16, 2013, 2:21 pm

IntegraXor, a manufacturer of supervisory control and data acquisition (SCADA) equipment, **announced last week** that it would implement a bug bounty program offering points redeemable for company services to researchers that disclose security vulnerabilities in their IGX SCADA system.

<http://threatpost.com/scada-vendor-offers-store-credit-for-vulnerabilities>

Issue \ System	IGX Backend	IGX Frontend	Project Editor	Inkscape/SAGE	Browser *	Plugin
Security Vulnerability	8k	8k	1k	128	128	0
Program Crash	1k	1k	1k	128	128	0
Program Hang	1k	1k	1k	128	128	0

<https://twitter.com/cBekrar/status/356550864212725760>

 **Chaouki Bekrar**  
@cBekrar [Follow](#)

Vendor bug bounty programs are shit & a SCADA vendor did even worst: "we pay off points to use our software license"  
[bit.ly/15vdrZJ](http://bit.ly/15vdrZJ)

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

<https://twitter.com/csoghoian/status/356560591801942016>

 **Christopher Soghoian**  
@csoghoian [Follow](#)

For once, I agree with @cBekrar. This SCADA vendor's o day bug bounty program is pathetic. Gift vouchers, not \$\$.  
[bit.ly/15vdrZJ](http://bit.ly/15vdrZJ)

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

28



ReVuln Ltd.

# The Bounty Program



- ⌘ The web server supports various commands, for:
  - ⌘ reading and writing files
  - ⌘ retrieving and setting the configuration
  - ⌘ reading data from the database
  - ⌘ login, logout
  - ⌘ alerts acknowledgement
  - ⌘ and so on.
- ⌘ One of these commands is `"/res"` which allows to load an arbitrary resource from an arbitrary DLL located in the program's main folder.

# Webserver commands



http://localhost:7131/DEM0/index.html ECAVA IntegraXor


Demo 2013-12-30 20:29:30 Login Guest

Plant Process Oil and Gas Transportat

About

registered

### License Information

 Warning: This computer program copyright law and international trade reproduction or distribution of this portion of it, may result in severe penalties, and will be prosecuted to the maximum under the law.


Sales Dept is hereby granting this software license project with the ID and title of **DEM0** and **Demo** purpose only. Do not use this as project template license registration. respectively, to IntegraXor Incubator 3 of Ecava Office at Technology Park of Bukit Jalil, Malaysia.

### License Registration

Version: IGX 4.1.4373.0  
 Serial Number: IGRX-2013-0208-14  
 Authorization Date: 2013-02-08 14:58:4

### Properties

General

 Powered by IntegraXor...

Protocol: HyperText Transfer Protocol  
 Type: HTML Document  
 Connection: Not Encrypted  
 Zone: Internet | Protected Mode: Off

Address (URL): [http://localhost:7131/DEM0/res?res/igres.dll/sys\\_about.html](http://localhost:7131/DEM0/res?res/igres.dll/sys_about.html)

Size: 4774 bytes

Created: 12/30/2013  
 Modified: 12/30/2013

Certificates

OK Cancel Apply

2013-12-30 20:19:44.041	Web Demo Server Started	10	10
2013-12-30 20:19:23.992	Checkpoint	0	

30



ReVuIn Ltd.

[http://localhost:7131/DEM0/res?res/igres.dll/sys\\_about.html](http://localhost:7131/DEM0/res?res/igres.dll/sys_about.html)

⌘ The syntax of the /res command is:

```
/PROJECT_NAME /res?  
DLL_NAME  
/RESOURCE_NAME
```

⌘ A stack buffer of 260 characters is used as destination for containing RESOURCE\_NAME with the result of a **stack based buffer-overflow**

# The /res command syntax



⌘ There is a **stack based buffer-overflow**

⌘ Affecting **igsvr.exe**  **igwebs.dll**

## The Issue





⌘ The pseudo-code of the /res handler is:

```
wchar_t buffer[260];           // MAX_PATH
...
buffer[0] = 0;
lstrcpyW(buffer, source);      // vulnerability
SplitPath(buffer);
```

## The /res handler (pseudo-code)



Command

ModLoad: 6e500000 6e570000 C:\Windows\SYSTEM32\wbemcomn.dll  
ModLoad: 6b1a0000 6b1ab000 C:\Windows\system32\wbem\wbemprox.dll  
ModLoad: 65270000 6528f000 C:\Windows\System32\wshom.ocx  
ModLoad: 64890000 648b9000 C:\Windows\System32\ScrRun.dll  
ModLoad: 6ad80000 6ad99000 C:\Windows\system32\wbem\wmiutils.dll  
ModLoad: 6ada0000 6adb0000 C:\Windows\system32\wbem\wbemsvc.dll  
ModLoad: 6adb0000 6ae72000 C:\Windows\system32\wbem\fastprox.dll  
(fc8.334): Break instruction exception - code 80000003 (first chance)  
\*\*\* ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\SYSTEM32\ntdll.dll -  
\*\*\* ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\KERNEL32.DLL -  
eax=7f533000 ebx=00000000 ecx=00000000 edx=7745a7c3 esi=00000000 edi=00000000  
eip=77381244 esp=0fb2f940 ebp=0fb2f96c iopl=0 nv up ei pl zr na pe nc  
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246  
ntdll!DbgBreakPoint:  
77381244 cc int 3  
0:088> g  
ig > 14:30.111 > [socket] select failed with error 0: The operation completed successfully.  
(fc8.b48): Access violation - code c0000005 (first chance exceptions are reported before this exception may be expected and handled).  
\*\*\* ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\ntdll.dll -  
eax=0b7ae180 ebx=00000008 ecx=00000061 edx=76bb682d esp=0b7ae0f4 ebp=0b7ae11c iopl=0  
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010202  
KERNEL32!lstrcpyW+0x1b:  
76bb682d 66890a mov word ptr [edx],cx  
0:023> d edx-10  
0b7afff0 61 00 61 00 61 00 61 00-61 00 61 00 61 00 61 00 a.a.a.a.a.a.a.a.  
0b7b0000 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??????????????  
0b7b0010 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??????????????  
0b7b0020 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??????????????  
0b7b0030 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??????????????  
0b7b0040 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??????????????  
0b7b0050 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??????????????  
0b7b0060 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??????????????  
0:023> gn  
ig > 14:44.051 > [socket] select failed with error 0: The operation completed successfully.  
(fc8.b48): Access violation - code c0000005 (!!! second chance !!!)  
eax=0b7ae180 ebx=00000008 ecx=00000061 edx=0b7b0000 esi=0be33ed8 edi=0be32058  
eip=76bb682d esp=0b7ae0f4 ebp=0b7ae11c iopl=0 nv up ei pl nz na po nc  
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010202  
KERNEL32!lstrcpyW+0x1b:  
76bb682d 66890a mov word ptr [edx],cx  
ds:0023:0b7b0000=????

IntegraXor Server

IntegraXor Server has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Close program

# DEMO TIME

35



ReVuln Ltd.

- ⌘ There are several ways to fix this issue
- ⌘ Using an IPS/IDS
- ⌘ Binary Patch
  - ⌘ **In-Memory** patch

## Fixing the issue





⌘ There are multiple ways, for example:

⌘ replace **lstrcpyW** with **StringCchCopyW**

⌘ **hook** the vulnerable function

## Fixing the issue - Binary Patch



& Security Vulnerabilities

& Uncovering new vulnerabilities

& Final considerations

# Agenda





- ⌘ There are **a lot of vulnerabilities** affecting SCADA/HMI solutions unknown to their users/vendors (as shown in the previous slides)
- ⌘ Vendors usually need a **long timeframe to fix** the issues, once these are reported to them (sometimes over a year, even if the issues have been reported to them)
- ⌘ Vendors **may not fix the issues** at all, and instead provide their users with some recommendations

# Final Considerations - I





- ⌘ There are only a few SCADA/HMI solutions having an **auto-update subsystem**
- ⌘ 99% of the cases an admin has to shutdown the system, install the patch, and restart the system
  - ⌘ This is **NOT acceptable**
- ⌘ The only way to circumvent this limitation is to rely on solutions like the one we tested (**DEMO'ed during S4 2013**) and included in SCADA shield:  
**Hot Patching**
  - ⌘ Issues **fixed without downtime**

## Final Considerations - II



- ⌘ There is the need for users to **explore and invest** in **new defensive solutions** such as SCADA shield
- ⌘ Solutions that **don't rely directly** on the Vendors
- ⌘ Waiting days for a security patch can be acceptable for Vendors, but **can't be acceptable** for SCADA/HMI users

## Final Considerations - III





revuln.com

info@revuln.com

twitter.com/revuln

# ReVuln Ltd.

*"Invincibility lies in the defense, the possibility of victory in the attack."*

# Thanks