

# Vulnerabilities in some SCADA Server Softwares

Luigi Auriemma

Dan Goodin

The following are almost all the vulnerabilities I found for a quick experiment some months ago in certain well known server-side SCADA softwares still vulnerable in this moment.

In case someone doesn't know SCADA (like me before the tests): it's just one or more softwares (usually a core, a graphical part and a database) that allow people to monitor and control the various hardware sensors and mechanisms located in industrial environments like nuclear plants, refineries, gas pipelines, airports and other less and more critical fields that go from the energy to the public infrastructures and obviously also the small "normal" industries.

In technical terms the SCADA software is just the same as any other software used everyday, so with inputs (in this case they are servers so the input is the TCP/IP network) and vulnerabilities: stack and heap overflows, integer overflows, arbitrary commands execution, format strings, double and arbitrary memory frees, memory corruptions, directory traversals, design problems and various other bugs.

Full-disclosure advisories and proof-of-concepts:

Siemens Tecnomatix FactoryLink:

[http://aluigi.org/adv/factorylink\\_1-adv.txt](http://aluigi.org/adv/factorylink_1-adv.txt)  
[http://aluigi.org/adv/factorylink\\_2-adv.txt](http://aluigi.org/adv/factorylink_2-adv.txt)  
[http://aluigi.org/adv/factorylink\\_3-adv.txt](http://aluigi.org/adv/factorylink_3-adv.txt)  
[http://aluigi.org/adv/factorylink\\_4-adv.txt](http://aluigi.org/adv/factorylink_4-adv.txt)  
[http://aluigi.org/adv/factorylink\\_5-adv.txt](http://aluigi.org/adv/factorylink_5-adv.txt)  
[http://aluigi.org/adv/factorylink\\_6-adv.txt](http://aluigi.org/adv/factorylink_6-adv.txt) (DoS only)

Iconics GENESIS32 and GENESIS64:

[http://aluigi.org/adv/genesis\\_1-adv.txt](http://aluigi.org/adv/genesis_1-adv.txt)  
[http://aluigi.org/adv/genesis\\_2-adv.txt](http://aluigi.org/adv/genesis_2-adv.txt)  
[http://aluigi.org/adv/genesis\\_3-adv.txt](http://aluigi.org/adv/genesis_3-adv.txt)  
[http://aluigi.org/adv/genesis\\_4-adv.txt](http://aluigi.org/adv/genesis_4-adv.txt)  
[http://aluigi.org/adv/genesis\\_5-adv.txt](http://aluigi.org/adv/genesis_5-adv.txt)  
[http://aluigi.org/adv/genesis\\_6-adv.txt](http://aluigi.org/adv/genesis_6-adv.txt)  
[http://aluigi.org/adv/genesis\\_7-adv.txt](http://aluigi.org/adv/genesis_7-adv.txt)  
[http://aluigi.org/adv/genesis\\_8-adv.txt](http://aluigi.org/adv/genesis_8-adv.txt)  
[http://aluigi.org/adv/genesis\\_9-adv.txt](http://aluigi.org/adv/genesis_9-adv.txt)  
[http://aluigi.org/adv/genesis\\_10-adv.txt](http://aluigi.org/adv/genesis_10-adv.txt)  
[http://aluigi.org/adv/genesis\\_11-adv.txt](http://aluigi.org/adv/genesis_11-adv.txt)  
[http://aluigi.org/adv/genesis\\_12-adv.txt](http://aluigi.org/adv/genesis_12-adv.txt)  
[http://aluigi.org/adv/genesis\\_13-adv.txt](http://aluigi.org/adv/genesis_13-adv.txt)

7-Technologies IGSS (Interactive Graphical SCADA System):

[http://aluigi.org/adv/igss\\_1-adv.txt](http://aluigi.org/adv/igss_1-adv.txt)  
[http://aluigi.org/adv/igss\\_2-adv.txt](http://aluigi.org/adv/igss_2-adv.txt)  
[http://aluigi.org/adv/igss\\_3-adv.txt](http://aluigi.org/adv/igss_3-adv.txt)  
[http://aluigi.org/adv/igss\\_4-adv.txt](http://aluigi.org/adv/igss_4-adv.txt)  
[http://aluigi.org/adv/igss\\_5-adv.txt](http://aluigi.org/adv/igss_5-adv.txt)  
[http://aluigi.org/adv/igss\\_6-adv.txt](http://aluigi.org/adv/igss_6-adv.txt)  
[http://aluigi.org/adv/igss\\_7-adv.txt](http://aluigi.org/adv/igss_7-adv.txt)  
[http://aluigi.org/adv/igss\\_8-adv.txt](http://aluigi.org/adv/igss_8-adv.txt)

DATAC RealWin:

[http://aluigi.org/adv/realwin\\_2-adv.txt](http://aluigi.org/adv/realwin_2-adv.txt)

# Vulnerabilities in some SCADA Server Softwares

Luigi Auriemma

Dan Goodin

[http://aluigi.org/adv/realwin\\_3-adv.txt](http://aluigi.org/adv/realwin_3-adv.txt)

[http://aluigi.org/adv/realwin\\_4-adv.txt](http://aluigi.org/adv/realwin_4-adv.txt)

[http://aluigi.org/adv/realwin\\_5-adv.txt](http://aluigi.org/adv/realwin_5-adv.txt)

[http://aluigi.org/adv/realwin\\_6-adv.txt](http://aluigi.org/adv/realwin_6-adv.txt)

[http://aluigi.org/adv/realwin\\_7-adv.txt](http://aluigi.org/adv/realwin_7-adv.txt)

[http://aluigi.org/adv/realwin\\_8-adv.txt](http://aluigi.org/adv/realwin_8-adv.txt)

## Giant Bullseyes Painted on Industrial Control Software

The security of software used to control hardware at nuclear plants, gas refineries and other industrial settings is coming under renewed scrutiny as researchers released attack code exploiting dozens of serious vulnerabilities in widely used programs.

The flaws, which reside in programs sold by Siemens, Iconics, 7-Technologies, Datab, and Control Microsystems, in many cases make it possible for attackers to remotely execute code when the so-called supervisory control and data acquisition software is installed on machines connected to the internet. Attack code was released by researchers from two separate security camps over the past week.

"SCADA is a critical field but nobody really cares about it," Luigi Auriemma, one of the researchers, wrote in an email sent to *The Register*. "That's also the reason why I have preferred to release these vulnerabilities under the full-disclosure philosophy."

The vulnerability dump includes proof-of-concept code for at least 34 vulnerabilities in widely used SCADA programs sold by four different vendors. Auriemma said the majority of the bugs allow code execution, while others allow attackers to access sensitive data stored in configuration files and one makes it possible to disrupt equipment that uses the software. He included a complete rundown of the vulnerabilities and their corresponding PoC code in a post published on Monday to the Bugtraq mail list.

It came six days after a Moscow-based security firm called Gleg announced the availability of Agora SCADA+, which attempts to collect virtually all known SCADA vulnerabilities into a single exploit pack. The 22 modules include exploits for 11 zero-day vulnerabilities, said the company's Yuriy Gurkin in an email. It's not clear how much the package costs.

Gurkin said Gleg's website has come under sustained web attacks shortly after releasing the SCADA exploit pack.

"We have tried to switch to ddoshostingsolutions.com provider but in just 3 days were out of 500 GB traffic limit," he said. "Currently trying to solve this."

The vulnerability of SCADA systems had long been theorized, but it wasn't until last year that the world got an object lesson on just how susceptible they could be to attack. In July, researchers reported the discovery of a computer worm that attacked SCADA software sold by Siemens. Research later showed that the underlying Stuxnet exploit amounted to a "search-and-destroy weapon" built to take out Iran's Bushehr nuclear reactor.

SCADA software often runs on extremely old systems that are difficult to replace without causing disruptions to critical equipment. As a result, installing patches and upgrades is frequently avoided despite the obvious security benefits.