Tofino Security | SCADAhacker.com

White Paper

Version 1.0
Published March 28, 2011

Analysis of the 7-Technologies IGSS Security Vulnerabilities for Industrial Control System Professionals

Contents

Authors

Eric Byres, P. Eng., ISA Fellow
CTO, Byres Security Inc.
eric@byressecurity.com
www.tofinosecurity.com

Joel Langill, CEH, CPT, CCNA
CSO, SCADAhacker.com
joel@scadahacker.com
www.scadahacker.com

Executive Summary

A number of previously unknown security vulnerabilities in the 7-Technologies Interactive Graphics SCADA System (IGSS) product have been publically disclosed. The release of these vulnerabilities included proof-of-concept (PoC) exploit code.

The products affected, namely IGSS, is a Supervisory Control and Data Acquisition (SCADA) system. It is used in a wide range of industries, including water/wastewater, district heating, food & beverage, building automation, marine, oil & gas, metals & mining, traffic control, gas distribution, and electric utilities.

At a minimum, all but one of the disclosed vulnerabilities can be used to forcefully crash a system server, causing a denial-of-service condition and loss of view. Of more serious concern to the SCADA and industrial control systems (ICS) community is the fact that for two of these vulnerabilities, it is relatively simple to inject malicious code in the targeted host and then remotely execute commands to activate this payload.

Attacks using these vulnerabilities could be difficult to detect and prevent. All vulnerabilities expose the core communication application within the IGSS platform used to manage communication between various clients and services.

While we are currently unaware of any malware or cyber attacks taking advantage of these security issues, there is a risk that criminals or political groups may attempt to exploit them for either financial or ideological gain.

This White Paper summarizes the current known facts about these vulnerabilities. It also summarizes the actions that operators of SCADA and ICS systems can take to protect critical operations.

Vulnerability Details

What is it?

A total of eight (8) vulnerabilities were disclosed targeting the IGSS platform. Of the eight mentioned, seven (7) attempt to exploit the `IGSSdataServer.exe` application on TCP port 12401, while the remaining vulnerability exploits the `dc.exe` application on TCP port 12397. Both vulnerable applications are part of the IGSS application suite.

Five (5) of the vulnerabilities identified with the `IGSSdataServer.exe` application exploit single or multiple stack (buffer) overflows. One exploits a directory traversal vulnerability, and the remaining vulnerability is a bug related to string formatting issues.

The single vulnerability in the `dc.exe` application allows execution of arbitrary applications within the file system.

All except for the “string formatting” vulnerability can be remotely exploited, providing the attacker the potential to execute arbitrary malicious code on a targeted control system.

What can an attacker do with this information?

The public disclosure of these vulnerabilities included sample data files that can be used with freely available hacking tools (such as netcat) for sending custom data packets on a network. These sample data files provide enough information so that a moderately skilled attacker could create new files which leverage the vulnerabilities further. The most likely intent of such an attacker would be to create malicious payloads that can then be executed remotely.

Typical malicious payloads range from simple remote shells, to information and credential stealing, to advanced call-back applications that can be used to further compromise the target. Most of these payloads can easily be created with a framework such as Metasploit and then remotely injected into the target control system using the disclosed vulnerabilities.

How easy is it to use these vulnerabilities to attack a system?

The publically available data files and sample command scripts provided with the disclosure make it easy to perform a variety of attacks on the target system. The "directory traversal" vulnerability coupled with the "arbitrary command execution" vulnerability represent the simplest attacks which can cause the greatest impact.

Most of the stack overflow vulnerabilities will cause the affected service to terminate prematurely and cause a denial-of-service condition. To inject and execute additional code using these vulnerabilities would require the moderate to advanced skills needed to create the payload and incorporate into it the proof-of-concept (PoC) data files. Not all stack overflows have been confirmed to allow remote code execution.

Is exploit code publically available?

Yes, the exploit code, including source code, is available through various forums including:

http://aluigi.org/adv.htm
http://www.securityfocus.com/bid/46936
http://www.exploit-db.com/exploits/17024/

Are any known viruses/worms or attack tools using these vulnerabilities?

There are currently no known viruses/worms or attack tools currently using these vulnerabilities. In addition, there are no automated exploit modules (Immunity CANVAS/Agora, Metasploit, etc.) utilizing these vulnerabilities. However, this is likely to change rapidly based on the current high state of awareness regarding ICS security.

What are the potential consequences to SCADA and control systems?

A successful attack successfully exploiting two of the disclosed vulnerabilities will allow the attacker to either execute malicious code or perform unauthorized actions. Either of these could completely compromise the integrity of the control system. At a minimum, applications can be prematurely terminated resulting in a denial-of-service condition that could potentially impact the production environment under control of the SCADA system.

The IGSS Data Server is responsible for transmission of data between the IGSS server and the operator stations.

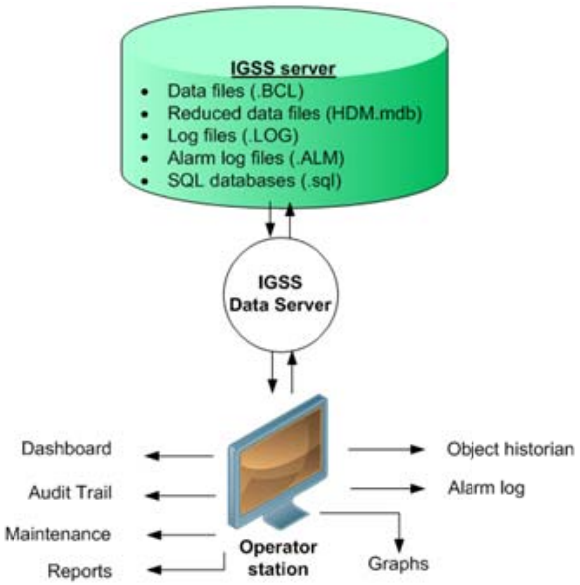

Figure 1: IGSS Data Server Communications

The only requirement for communication between the IGSS Data Server and an arbitrary client is an IP connection and access to a specific TCP/IP port. There is no authentication process in place on this connection, so a vulnerability in such a critical service could compromise the overall integrity of the system communications, leading to deeper system penetration and potential compromise of the underlying control system.

Affected Systems

What Control/SCADA Systems are affected?

The following control and SCADA systems are believed to be directly affected by these vulnerabilities:

- IGSS Version 9
- IGSS Version 8
- IGSS Version 7

7-Technologies has confirmed that Version 9 is affected by all eight (8) vulnerabilities, while Versions 7 and 8 are only vulnerable to exploits against the `dc.exe` application allowing remote execution of arbitrary code. Version 7 and older are not officially supported by the vendor. Sites using older, unsupported software should contact 7-Technologies Technical Support for information relating to system security.

Detection and Removal

Anti-virus products

Since this is not a virus/worm/Trojan, but rather a remote exploit, there are no known detection and/or removal products available. Certain anti-virus products are capable of detecting buffer overflow situations; however none have been specifically tested against these exploits. These products would have little impact on the directory traversal and file execution vulnerabilities until an updated specific virus signature is available.

Intrusion detection products

Emerging Threats Pro, with assistance from NitroSecurity, have developed Intrusion Detection System (IDS) signatures for all of the vulnerabilities noted in this white paper. These IDS signatures are also available in the Quickdraw SCADA IDS Vulnerability Ruleset.

Available Patches or Updates

On March 25, 2011, 7-Technologies announced that a patch for these vulnerabilities was available for registered IGSS end users (http://www.igss.com/company/news-and-press-center/11-03-25/IGSS_%e2%80%93_ongoing_focus_on_security.aspx?News=NewsItem).

A general Version 8 and 9 update is available on their website under the "Download" section (http://www.igss.com/download/licensed-versions.aspx). Previous versions of the IGSS software are considered by 7-Technologies to be "unsupported" and no updates have been provided.

We have been able to confirm that this general update corrects the vulnerabilities in Versions 8 and 9 software discussed in this paper.

Compensating Controls

Compensating controls are actions that will not correct the underlying issue, but will help block known attack vectors for systems where no patch is available or the patch has not yet been installed. Compensating controls also provide an additional level of security in critical systems where patches have been installed. The following are six suggested compensating controls for IGSS systems:

1. Installation of Industrial Firewalls to Protect Server

Several of these vulnerabilities represent a significant risk to the integrity of the IGSS system, and could potentially compromise the system entirely using simple attack techniques. Furthermore, they are difficult to detect or prevent as they are using "valid" communications with the targeted IGSS server.

This firewall should be implemented with a rule set that allows traffic only from other authorized IGSS hosts using the specific services/ports needed for the IGSS product to operate. To determine the port needed, contact your 7-Technologies representative or use a firewall offering automated learning features.

The use of industrial firewalls is recommended due to the high-risk exposure of these services from not only less-trusted remote networks, but also the local trusted control system network[i].

2. Minimize Network Exposure of Vulnerable Systems

Due to the extent of these vulnerabilities, and how they can impact both the primary communications infrastructure of the IGSS environment, as well as unrestricted access to the file system on the server (potentially allowing a complete compromise of the server), external or remote access from less-trusted networks should be severely restricted or eliminated. Less-trusted networks include both public networks like the Internet, as well as general-purpose office networks, which may have access to the Internet.

If external communications are required, industrial firewalls should be utilized between networks, and should contain rule sets that severely limit the external hosts that are allowed to communicate with the IGSS hosts. For the allowed hosts, communications should be restricted to just the services/ports which are used in critical communications. Considerable security risk is present if host-to-host communication is filtered on IP address alone, so additional port/service rules are essential.

3. Install an Intrusion Detection System

IDS systems are monitoring systems designed to detect network messages that match known vulnerability signatures. As noted earlier, a number of IDS vendors have released signatures for the vulnerabilities affecting the IGSS products. We strongly recommend that users of the IGSS product install an IDS product on their control network and monitor it regularly.

4. Regularly Check System Log Files

Until the vendor patch is installed and validated, all system log files, especially those contained within the Windows operating system, should be checked regularly and reviewed for any unexpected termination of applications and services. These could be a sign that a remote attack is being attempted.

5. Regularly Check Security Perimeter Device Log Files

Significant information can be determined by looking at log files in perimeter devices (such as firewalls), paying particular attention to “denied” access attempts to the trusted control system network using either TCP/12401 or port TCP/12397. These failed attempts could point to a potential attacker trying to exploit the vulnerabilities.

---

[i] The Tofino Security Appliance installed with the Tofino Firewall and Tofino Secure Asset Management LSMs (Loadable Software Modules) is specifically designed to provide this level of protection from unknown threats. If OPC communications is used in the control network, then the Tofino OPC Enforcer LSM is also recommended. For additional details see: http://www.tofinosecurity.com/products.

6. Monitor Vendor Support Site for Applicable Patches

These vulnerabilities are expected to extend beyond a broad range of software releases. This could mean that many sites are not covered under current support contracts, and are unable to download patches as they become available. In all cases, we recommend that users contact their local 7-Technologies representative for instructions on distribution and installation of the patches as they become available.

Frequently Asked Questions

What is a Directory Traversal Vulnerability?

Directory Traversal (or path traversal) is a type of security exploit that involves the use of characters designed to induce a “traverse to parent directory” typically within a web server, but can also occur with applications using APIs. This exploit is used to gain access to files or directories that would otherwise be restricted. The access granted by a Directory Traversal vulnerability may simply allow read-only access to files, as well as complete read-write-execute-delete capabilities.

Directory Traversal typically occurs as a result of insufficient security validation/sanitization of user-supplied input allowing characters representing "traverse to parent directory" through to the file APIs. This attack exploits poor security design (i.e. the software is acting as it is supposed to, but the full consequences have not been considered) as opposed to exploiting a bug in the code.

What is a Stack Overflow Vulnerability?

A *Stack Overflow* occurs when the results from a valid operation create a result that is larger than that which can be managed by the memory space allocated, often resulting in memory corruption. This is typically caused by the application code failing to validate user input prior to processing. A successful exploit could allow additional malicious code to be executed. Unsuccessful exploit attempts will likely result in the premature termination of the application leading to a denial-of-service condition.

What does it mean to allow Arbitrary Command Execution?

Arbitrary Command (or Code) Execution is a type of vulnerability similar to Directory Traversal with the added ability of allowing commands to be sent to the vulnerable host remotely using a command string that closely represents the dot-dot-slash format. This type of vulnerability could allow the attacker to execute commands that would otherwise be prohibited without elevated privileges. The commands can execute both built-in “shell” commands, as well as other files that may exist on the file system such as batch files, executables, shell code, and “net” commands.

Who is 7-Technologies and what is their IGSS product?

7-Technologies was founded in 1984 and is an independent software provider based in Denmark, providing monitoring and control systems that are used primarily in Europe and South Asia. Their business is built on a strategy whereby software is sold and implemented through a network of more than 200 global partners and system integrators.

IGSS is a SCADA system found in a wide range of industries, including water/wastewater, district heating, food & beverage, building automation, marine, oil & gas, metals & mining, traffic control, gas distribution, and electric utilities. According to the 7-Technologies website, the company has sold more than 28,000 IGSS licenses in 50 countries since the product was first introduced in 1984.

What is a zero-day vulnerability?

Zero-day vulnerabilities or “0 days” (pronounced “oh days”) are those that are unpatched by the affected software’s manufacturer. The “days” start counting once a patch is publically released.

I don't use the versions of IGSS listed on the BugTrak site – do I still need to be concerned?

Initial analysis seems to indicate that these vulnerabilities only affect IGSS Versions 8 and 9. This is due primarily to the fact that these vulnerabilities focus on a single `IGSSdataServer` application that is not believed to have existed in prior versions of the software. Until the vendor has posted an official response to these vulnerabilities, increased security diligence should be used based on the recommendations provided in this document.

References

For more information about this issue, see the following references:

7-Technologies

Product Support

http://www.igss.com/support/support.aspx

http://www.igss.com/company/news-and-press-center/11-03-25/IGSS_%e2%80%93_ongoing_focus_on_security.aspx?News=NewsItem

White Papers and Application Notes

http://www.tofinosecurity.com/professional/good-practice-guide-firewall-deployment-scada-and-process-control-networks

http://www.tofinosecurity.com/professional/securing-your-opc-classic-control-system

http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

IDS Signatures

http://www.digitalbond.com/tools/quickdraw/vulnerability-rules/

http://blog.emergingthreatspro.com/2011/03/emerging-threats-pro-scada-sigs.html

US-CERT

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-080-03.pdf

CVE References

As of March 27, 2011, these vulnerabilities have not been listed with CVE.

Acknowledgements and Trademarks

The vulnerabilities noted in this paper were publically reported by Luigi Auriemma on March 21, 2011 http://aluigi.org/

The image used in Figure 1 is from online documentation for the IGSS Data Server, available at: http://www.igss.com/overview/version-overview/new-features-in-version9/igss-data-server.aspx

Non-Affiliated Trademarks

Affiliated Trademarks