WHITEPAPER ON SECURITY VULNERABILITIES 2020 V10

JUNE 2020

An ICONICS Whitepaper

CONTENTS

100 Foxborough Blvd., Foxborough, MA 02035

1 Overview

ICONICS takes extraordinary efforts in testing and validating all software before it is released. Unfortunately, we have had instances where external researchers have discovered vulnerabilities in our products. ICONICS takes such issues very seriously. Within hours of becoming aware of these issues, ICONICS assigns engineering teams to validate, and then to quickly resolve, those vulnerabilities that are valid.

For each proven vulnerability, patches are quickly developed and, once fully tested, are posted at the following Web site for all current releases and, in some cases, past releases.

http://www.iconics.com/certs

ICONICS coordinates with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on these issues, as requested.

The following table lists all vulnerabilities that are described in this document. This document is updated when a new issue is reported and validated to be true.

Section	Vulnerability Issue
2	GenBroker Buffer Overflow (ICS-Alert-11-080-02).
3	SafeNet Licensing Driver (ICS-CERT Advisory 11-108-01))
4	GenBroker Out of Bounds (ICS-CERT Advisory ICSA-20-170-03)
5	GENESIS64™ Denial of Service (ICS-CERT Advisory ICSA-20-170-03)
6	GENESIS64 Workbench RCE (ICS-CERT Advisory ICSA-20-170-03)
7	GENESIS64 Information Disclosure (ICS-CERT Advisory ICSA-20-170-03)
8	GENESIS64 RCE (ICS-CERT Advisory ICSA-20-170-03)

ICONICS GENESIS64™ software is used by customers to provide manufacturing, process and building automation solutions for their operations. Currently, installed applications include manufacturing, building automation, oil & gas, water/wastewater, utilities (including renewable) and others. The products are used globally with an estimated distribution of 55 percent in the USA, 40 percent in Europe, and 5 percent in Asia.

ICONICS recommends that users of its products (GENESIS64, Hyper Historian™, AnalytiX®, and MobileHMI™) take the following steps to prevent potential cybersecurity vulnerabilities:

- Use a firewall. Place control system networks, devices, and SCADA system components behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Use a VPN for remote access to control system devices.

2 GenBroker (ICS-CERT ALERT 11-080-02)

2.1 Issue – Discussion

On March 21, 2011, US-CERT informed ICONICS of a researcher's claim of a potential vulnerability in the GenBroker component in the ICONICS' GENESIS32™ and GENESIS64 products.

ICONICS validated the researcher's claims for the 9.21 and 10.51 versions and has released downloadable patches, as well as the steps listed below, to further mitigate the vulnerabilities. The patches for 9.21 and 10.51 can be downloaded at the ICONICS Support Web site.

ICONICS has coordinated with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on this issue.

2.2 Products Affected

The following table identifies currently-supported ICONICS products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
GenBroker contained in the products: • GENESIS32 • BizViz	All version up to an including V9.2	Denial of Service Possible remote code execution	High
GenBroker64 contained in the Products: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including V10.51	Denial of Service Possible remote code execution	High

2.3 Impact

A successful exploit of the GenBroker (buffer overflow or memory corruption) vulnerability could allow a denial of service (DOS) or arbitrary code execution. The specific impact to an organization depends on many factors unique to that organization. ICONICS recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

2.4 Vulnerability

The vulnerability discovered exists in GenBroker: an OPC-based communications program that runs as a service as part of the GENESIS32, BizViz, and GENESIS64 products. The service utilizes TCP Port 38080 as part of its normal communications. It is vulnerable to invalid and unintended messages directed to the port, receipt of which can cause buffer overflow or memory corruption, either of which can result in a denial of service and/or a GenBroker crash. This vulnerability is remotely exploitable and exploit code has been released.

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT:
Exploit code specifically targeting this vulnerability has been released.

DIFFICULTY:
An attacker would require at least an advanced skill level to exploit these vulnerabilities. The Denial of Service vulnerability exploit would require development of a malicious application with access to TCP port 38080 on the server machine running GenBroker and an understanding of the protocol used on that port. The malicious application would need to send an invalid and specifically targeted message that overflows the internal buffer or frees initialized memory pointers.

2.5 Mitigation

ICONICS is releasing updated versions of GenBroker for GENESIS32 and BizViz versions 8.05, 9.01, 9.13, 9.21, and for GENESIS64 version 10.51 that properly discards invalid messages directed to it.

ICONICS recommends that users of GENESIS32, BizViz, and GENESIS64 take the following mitigation steps:

- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Restrict access to TCP Port 38080. If remote access is required, utilize secure methods such as Virtual Private Networks (VPNs).
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Install the patch.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its Web site at http://www.iconics.com/certs. ICONICS is committed to providing high-quality secure products to its customers.

Organizations should follow their established internal procedures if they observe suspected malicious activity and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures. The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

3 SafeNet Licensing Driver (ICS-CERT Advisory 11-108-01)

3.1 Issue – Discussion

This vulnerability exists in the SafeNet Sentinel Protection Server v7.3.3, a third-party software component executing the Sentinel License key function, and utilized in the GENESIS32, GENESIS64 and BizViz products. This version of the SafeNet Sentinel Protection Server utilizes a "hidden" Web service running on port TCP/6002. This service is classified as "hidden" due to the fact that it does not easily expose itself when the Windows Firewall is enabled.

Additional information on this vulnerability can be found in the NIST National Vulnerability Database (CVE-2007-6483), where it is revealed that versions 7.0.0 through 7.4.0 were vulnerable to a directory traversal attack, allowing unrestricted access to a large portion of the file system, compromising data integrity and access to key files.

3.2 Products Affected

The following table identifies currently-supported ICONICS products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
GENESIS32, BizViz	All versions up to and including V9.2	Directory Transversal	Medium
GENESIS64, Hyper Historian	All versions up to and including V10.51	Directory Transversal	Medium

3.3 Impact

A successful exploit of the Licensing (directory traversal) vulnerability could allow access to a portion of the file system, compromising data integrity and access to key files. The specific impact to an organization depends on many factors unique to that organization. ICONICS recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

3.4 Vulnerability

This vulnerability exists in the SafeNet Sentinel Protection Server v7.3.3, a third-party software component executing the Sentinel License key function, and utilized in ICONICS GENESIS32, GENESIS64 and BizViz products. This version of the SafeNet Sentinel Protection Server utilizes a "hidden" Web service running on port TCP/6002. This service is classified as "hidden" due to the fact that it does not easily expose itself when the Windows Firewall is enabled.

Additional information on this vulnerability can be found in the NIST National Vulnerability Database (CVE-2007-6483), where it is revealed that versions 7.0.0 through 7.4.0 were vulnerable to a directory traversal attack, allowing unrestricted access to a large portion of the file system, compromising data integrity and access to key files.

EXPLOITABILITY:
These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT:
Exploit code specifically targeting this vulnerability has been released.

DIFFICULTY:
An attacker would require at least an advanced skill level to exploit these vulnerabilities. An exploit of the license key vulnerability would require an attacker to develop a specially crafted message and send this message to the SafeNet Sentinel License Monitor server port (6002/TCP).

3.5 Mitigation

ICONICS has released an updated version of the SafeNet Sentinel Protection Server (v7.6.4) that addresses the directory traversal vulnerability.

ICONICS recommends that users of GENESIS32, BizViz, and GENESIS64 take the following mitigation steps:

- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Restrict access to TCP Port 6002. If remote access is required, utilize secure methods such as Virtual Private Networks (VPNs).
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Install the patch.

Organizations should follow their established internal procedures if they observe suspected malicious activity and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures. The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

4 GENESIS64 GenBroker OOB (ICS-CERT Advisory ICSA-20-170-03)

4.1 Issue – Discussion

On January 21, 2020, researchers Tobias Scharnowski, Niklas Breitfeld, and Ali Abbasi reported a potential security vulnerability in the GENESIS64 GenBroker64 module.

ICONICS validated the researcher's claims that GenBroker64 is susceptible to an Out of Bounds condition which, if exploited, can result in remote code execution. ICONICS has released a set of downloadable patches for this vulnerability, as well as steps listed below to mitigate this vulnerability. Patches are available for several versions of GENESIS64 and for GENESIS32, which also has this vulnerability. These patches can be downloaded from the ICONICS web site, http://www.iconics.com/certs.

ICONICS has coordinated with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on this issue. ICS-CERT assigned CVE-2020-12011 to this vulnerability.

4.2 Products Affected

The following table identifies currently-supported ICONICS products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
GenBroker64 contained in the products: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including V10.96	Out of Bounds Possible remote code execution	A CVSS base score of 8.1 was calculated

4.3 Impact

A successful exploit of GenBroker64 can potentially result in remote code execution.

The specific impact to an organization depends on many factors unique to that organization. ICONICS recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

4.4 Vulnerability

Exploitation of the GenBroker64 vulnerability requires creation of a specially crafted communication packet which must be sent to GenBroker's IP Address and Port Number.

EXPLOITABILITY:

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT
There is no known exploit code specifically targeting this vulnerability other the code created to demonstrate the vulnerability by the researcher.

DIFFICULTY
An attacker would need a very high skill level to be able to exploit this vulnerability. It requires determining the Out of Bounds condition that GenBroker is vulnerable to, and requires crafting of a special communications packet to take advantage of it.

4.5 Mitigation

ICONICS is releasing a patch for GenBroker64 for the versions V10.96, V10.95.5, and V10.95.2.

ICONICS recommends that users of its products take the following mitigation steps:

- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Do not click Web links or open unsolicited attachments in e-mail messages.
- Install the patch.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its web site at http://www.iconics.com/certs. ICONICS is committed to providing high-quality secure products to its customers. Organizations should follow their established internal procedures if they observe suspected malicious activity and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures. The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

5 GENESIS64 DoS (ICS-CERT Advisory ICSA-20-170-03)

5.1 Issue – Discussion

On January 21, 2020, Yehuda Anikster of Claroty Research reported a potential security vulnerability in GENESIS64 which can result in a Denial of Service (DoS).

ICONICS validated the researcher's claim that GENESIS64 has a flawed deserialization algorithm that, if exploited, makes GENESIS64 susceptible to a DoS attack.

ICONICS has released a set of downloadable patches for this vulnerability, as well as steps listed below to mitigate this vulnerability. Patches are available for several versions of GENESIS64 for this vulnerability. These patches can be downloaded from the ICONICS website, http://www.iconics.com/certs.

ICONICS has coordinated with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on this issue. ICS-CERT assigned CVE-2020-12015 to this vulnerability.

5.2 Products Affected

The following table identifies currently-supported ICONICS products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
Platform Services contained in the products: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including V10.96	Denial of Service	A CVSS base score of 7.5 was calculated

5.3 Impact

A successful exploit of this deserialization issue can potentially result in a crash of the software and denial of service.

The specific impact to an organization depends on many factors unique to that organization. ICONICS recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

5.4 Vulnerability

Exploitation of this deserialization issue requires creation of a specially crafted communication packet which must be sent to the GENESIS64 Platform Services.

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT
There is no known exploit code specifically targeting this vulnerability other the code created to demonstrate the vulnerability by the researcher.

DIFFICULTY
An attacker would need a moderately high skill level to be able to exploit this vulnerability. It requires determining the deserialization issue and requires crafting of a special communications packet to take advantage of it.

5.5 Mitigation

ICONICS is releasing patches for the versions V10.96, V10.95.5, and V10.95.2 of its products.

ICONICS recommends that users of its products take the following mitigation steps:

- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Do not click Web links or open unsolicited attachments in e-mail messages.
- Install the patch.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its web site at http://www.iconics.com/certs. ICONICS is committed to providing high-quality secure products to its customers.

Organizations should follow their established internal procedures if they observe suspected malicious activity and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures. The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

6 GENESIS64 Workbench RCE (ICS-CERT Advisory ICSA-20-170-03)

6.1 Issue – Discussion

On January 21, 2020, researchers Pedro Ribeiro and Radek Domanski of Flashback reported a potential security vulnerability in GENESIS64 Workbench which can result in Remote Code Execution if exploited.

ICONICS validated the researcher's claim that GENESIS64 Workbench was not enforcing security on certain project files and that, if exploited, made GENESIS64 susceptible to a remote code execution attack.

ICONICS has released a set of downloadable patches for this vulnerability, as well as steps listed below to mitigate this vulnerability. Patches are available for several versions of GENESIS64 for this vulnerability. These patches can be downloaded from the ICONICS web site, http://www.iconics.com/certs.

ICONICS has coordinated with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on this issue. ICS-CERT assigned CVE-2020-12009 to this vulnerability.

6.2 Products Affected

The following table identifies currently-supported ICONICS products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
Workbench contained in the products: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including V10.96	Possible Remote Code Execution	A CVSS base score of 7.5 was calculated

6.3 Impact

A successful exploit of this vulnerability can potentially result in remote code execution.

The specific impact to an organization depends on many factors unique to that organization. ICONICS recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

6.4 Vulnerability

Exploitation of this deserialization issue requires creation of a specially crafted package file for the GENESIS64 Workbench Pack-and-Go function.

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT
There is no known exploit code specifically targeting this vulnerability other the code created to demonstrate the vulnerability by the researcher.

DIFFICULTY
An attacker would need a moderate skill level to be able to exploit this vulnerability. It requires knowledge of the GENESIS64 Workbench package file format and requires the crafting of a special package to take advantage of it.

6.5 Mitigation

ICONICS is releasing patches for the versions V10.96, V10.95.5, and V10.95.2 of its products.

ICONICS recommends that users of its products take the following mitigation steps:

- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Do not click Web links or open unsolicited attachments in e-mail messages.
- Install the patch.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its web site at http://www.iconics.com/certs. ICONICS is committed to providing high-quality secure products to its customers.

Organizations should follow their established internal procedures if they observe suspected malicious activity and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures. The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

7 GENESIS64 Info Disclosure (ICS-CERT Advisory ICSA-20-170-03)

7.1 Issue – Discussion

On January 22, 2020, researcher Ben McBride of Oak Ridge National Laboratory reported a potential security vulnerability in GENESIS64 V10.95 which can result in information disclosure if exploited.

ICONICS validated the researcher's claim that in GENESIS64 V10.95, the GridWorX Server function can be abused to exfiltrate the contents of a database, modify data, and, in some configurations, execute commands. It should be noted, this vulnerability does not exist in the latest version of GENESIS64 (V10.96).

ICONICS has released a set of downloadable patches for this vulnerability, as well as steps listed below to mitigate this vulnerability. Patches are available for several versions of GENESIS64 for this vulnerability. These patches can be downloaded from the ICONICS web site, http://www.iconics.com/certs.

ICONICS has coordinated with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on this issue. ICS-CERT assigned CVE-2020-12013 to this vulnerability.

7.2 Products Affected

The following table identifies currently-supported ICONICS products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
FrameWorX Server contained in the products: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including V10.95.5	Information Disclosure Possible Execution of Commands, depending on system setup	A CVSS base score of 9.4 was calculated

7.3 Impact

A successful exploit of this vulnerability can potentially result in information disclosure, modify data, and possible execution of commands, depending on how the system is setup.

The specific impact to an organization depends on many factors unique to that organization. ICONICS recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

7.4 Vulnerability

Exploitation of this security issue requires creation of a custom WCF client that interfaces to the GridWorX point manager and the execution of certain arbitrary SQL commands remotely.

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT
There is no known exploit code specifically targeting this vulnerability other the code created to demonstrate the vulnerability by the researcher.

DIFFICULTY
An attacker would need a moderate skill level to be able to exploit this vulnerability. It requires understanding of certain GENESIS64 GridWorX methods and the ability to develop a custom WCF client that can take advantage of the vulnerability.

7.5 Mitigation

ICONICS is releasing patches for the versions V10.95.5 and V10.95.2 of its products. ICONICS recommends that users of its products take the following mitigation steps:

- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Do not click Web links or open unsolicited attachments in e-mail messages.
- Install the patch.
- Reduce the database permissions for the user account running the ICONICS GridWorX Point Manager to the minimal set necessary to perform the required functionality. If no database access is required from GENESIS64 it is recommended to disable the service.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its web site at http://www.iconics.com/certs. ICONICS is committed to providing high-quality secure products to its customers. Organizations should follow their established internal procedures if they observe suspected malicious activity and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures. The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

8 GENESIS64 RCE (ICS-CERT Advisory ICSA-20-170-03)

8.1 Issue – Discussion

On January 21, 2020, researchers Steven Seeley and Chris Anastasio of Incite reported a potential security vulnerability in GENESIS64 which can result in Remote Code Execution, if exploited.

ICONICS validated the researcher's claim that a deserialization issue in GENESIS64 FrameWorX Server could, if exploited, make GENESIS64 susceptible to a remote code execution attack.

ICONICS has released a set of downloadable patches for this vulnerability, as well as steps listed below to mitigate this vulnerability. Patches are available for several versions of GENESIS64 for this vulnerability. These patches can be downloaded from the ICONICS web site, http://www.iconics.com/certs.

ICONICS has coordinated with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on this issue. ICS-CERT assigned CVE-2020-12007 to this vulnerability.

8.2 Products Affected

The following table identifies currently-supported ICONICS products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
FrameWorX Server contained in the following products: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including V10.96	Possible Remote Code Execution	A CVSS base score of 7.5 was calculated

8.3 Impact

A successful exploit of this vulnerability can potentially result in remote code execution.

The specific impact to an organization depends on many factors unique to that organization. ICONICS recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

8.4 Vulnerability

Exploitation of this deserialization issue requires creation of a specially crafted communications packet for FrameWorX Server within GENESIS64.

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT
There is no known exploit code specifically targeting this vulnerability other the code created to demonstrate the vulnerability by the researcher.

DIFFICULTY
An attacker would need a high skill level to be able to exploit this vulnerability. It requires attaining knowledge of the GENESIS64 FrameWorX Server communications and its deserialization, and being able to craft a special communications packet that takes advantage of a specific shortcoming in the deserialization.

8.5 Mitigation

ICONICS is releasing patches for the versions V10.96, V10.95.5, and V10.95.2 of its products.

ICONICS recommends that users of its products take the following mitigation steps:

- Use a firewall. Place control system networks and devices behind firewalls and isolate them from the business network.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Do not click Web links or open unsolicited attachments in e-mail messages.
- Install the patch.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its web site at http://www.iconics.com/certs. ICONICS is committed to providing high-quality secure products to its customers. Organizations should follow their established internal procedures if they observe suspected malicious activity and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures. The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber security with Defense-in-Depth Strategies.

Founded in 1986, ICONICS is an award-winning independent software provider offering real-time visualization, HMI/SCADA, energy management, fault detection, manufacturing intelligence, MES, and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70 percent of the Global 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality, and to be more sustainable.

ICONICS is leading the way in cloud-based solutions with its HMI/SCADA, analytics, mobile and data historian to help its customers embrace the Internet of Things (IoT). ICONICS products are used in manufacturing, building automation, oil and gas, renewable energy, utilities, water and wastewater, pharmaceuticals, automotive, and many other industries. ICONICS' advanced visualization, productivity, and sustainability solutions are built on its flagship products: GENESIS64™ HMI/SCADA, Hyper Historian™ plant historian, AnalytiX® solution suite, and MobileHMI™ mobile apps. Delivering information anytime, anywhere, ICONICS' solutions scale from the smallest standalone embedded projects to the largest enterprise applications.

ICONICS promotes an international culture of innovation, creativity, and excellence in product design, development, technical support, training, sales, and consulting services for end users, systems integrators, OEMs, and channel partners. ICONICS has over 350,000 applications installed in multiple industries worldwide.

World Headquarters
100 Foxborough Blvd.
Foxborough, MA, USA, 02035
+1 508 543 8600
us@iconics.com

European Headquarters
Netherlands
+31 252 228 588
holland@iconics.com

Australia
+61 2 9605 1333
australia@iconics.com

Canada
+1 647 544 1150
canada@iconics.com

China
+86 10 8494 2570
china@iconics.com

Czech Republic
+420 377 183 420
czech@iconics.com

France
+33 4 50 19 11 80
france@iconics.com

Germany
+49 2241 16 508 0
germany@iconics.com

India
+91 265 6700821
india@iconics.com

Italy
+39 010 46 0626
italy@iconics.com

Middle East
+966 540 881 264
middleeast@iconics.com

Singapore
+65 6667 8295
singapore@iconics.com

UK
+44 1384 246 700
uk@iconics.com

Winner
Microsoft Partner
2018 Partner of the Year
Manufacturing Award

Gold
Microsoft Partner

VISUALIZE HISTORIZE MOBILIZE ANALYZE IoT CLOUD