WHITEPAPER ON ICONICS SUITE SECURITY VULNERABILITIES – DECEMBER 2022

An ICONICS Whitepaper

100 Foxborough Blvd., Foxborough, MA 02035

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 website for all current releases and, in some cases, past releases.

http://iconics.com/cert

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	FWX Server Faulty String Deserialization (ICS-CERT Advisory ICSA-20-170-03)
6	FWX Server Deserialization (ICS-CERT Advisory ICSA-20-170-03)
7	Security not enforced on Project Files (ICS-CERT Advisory ICSA-20-170-03)
8	Security missing on Procedures and Datasets (ICS-CERT Advisory ICSA-20-170-03)
9	OPC UA Framework Uncontrolled Recursion (ICS-CERT Advisory ICSA-21-294-03)
10	GraphWorX64 AutoCAD Import OOB (ICS-CERT Advisory ICSA 21-294-01)
11	Cross Site Scripting (ICS-CERT Advisory ICSA 22-020-01)
12	Incomplete List of Disallowed Inputs (ICS-CERT Advisory ICSA 22-020-01)
13	Plaintext Storage of Password (ICS-CERT Advisory ICSA 22-020-01)
14	Buffer Over-read (ICS-CERT Advisory ICSA 22-020-01)
15	MobileHMI Directory Traversal (ICS-CERT Advisory ICSA-22-202-04)
16	XAML/XML Deserialization (ICS-CERT Advisory ICSA-22-202-04)
17	GraphWorX64 Scripting (ICS-CERT Advisory ICSA-22-202-04)
18	GenBroker Deserialization (ICS-CERT Advisory ICSA-22-202-04)
19	GenBroker Out-of-Bounds Read (ICS-CERT Advisory ICSA-22-202-02)
20	Path Traversal in Workbench (ICS-CERT Advisory ICSA-22-347-01)
21	OpenSSL Buffer Overrun in BACnet/SC

The following table is a summary of what updates or patched files are necessary to bring the given version as up to date as possible with regards to protecting the system against the vulnerabilities described in this document.

ICONICS software version	**Is not subject to these vulnerabilities…**	**…After applying this update pack or these patch files…**	**…With this date/version or later**
10.97.2	All in this document	10.97.2 Critical Fixes Rollup	Rollup 1
10.97.1	Up to and including section 19	10.97.1 Critical Fixes Rollup	Rollup 3
10.97	Up to and including section 14	10.97 Critical Fixes Rollup	Rollup 2
10.96.2	Up to and including section 9, plus section 11 and 13	10.96.2 Critical Fixes Rollup	Rollup 2
10.96.1	Up to and including section 8, plus section 11 and 13	10.96.1 Critical Fixes Rollup	Rollup 3
10.96	Up to and including section 8, plus section 13	10.96 Critical Fixes Rollup	Rollup 5
10.95.5	Up to and including section 9	FwxAsyncCore.dll FwxIotJsonEncoderDecoder.dll FwxServerCore.dll GdxPointManager.dll GenBroker64.exe IcoConfigCommon.dll IcoConfigCommonAG.dll IcoConfiguratorCore.dll IcoEaClient.dll IcoEaConfiguration.dll IcoEaDefinitions.dll IcoEaPowershell.dll IcoGdxClient.dll IcoGdxDefinitions.dll IcoHHClient.dll IcoHHConfiguration.dll IcoWorkbenchConfiguration.dll IcoWorkbenchCore.dll IcoWorkbenchDefinitions.dll IcoWorkbenchPackAndGo.dll Opc.Ua.Core.dll	2020-05-07 1.03.340.2

10.95.2	Up to and including section 8, plus section 12	FwxAsyncCore.dll FwxIotJsonEncoderDecoder.dll FwxServerCore.dll GenBroker64.exe IcoCommon.dll IcoConfigCommon.dll IcoConfigCommonAG.dll IcoConfiguratorCore.dll IcoEaClient.dll IcoEaConfiguration.dll IcoEaDefinitions.dll IcoEaPowershell.dll IcoHHClient.dll IcoHHConfiguration.dll IcoWorkbenchConfiguration.dll IcoWorkbenchCore.dll IcoWorkbenchDefinitions.dll IcoWorkbenchPackAndGo.dll	2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-30 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27 2020-03-27
10.9	Up to and including section 3, plus section 12	None required.	
10.8	Up to and including section 3, plus section 12 and 13	None required.	
10.7	Up to and including section 3, plus section 12 and 13	None required.	
10.6	Up to and including section 3, plus section 12 and 13	None required.	
10.51	Up to and including section 3, plus section 12 and 13	10.51 Hot Fix Pack	Hot Fix Pack 1

ICONICS recommends that users of its products (ICONICS Suite, 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.

Acronyms and Terms used in this document:

Term	Definition
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration

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

2.1 Date: May 2011

2.2 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 website.

2.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product and Component	Version	Security Impact	Severity Rating
GenBroker64 contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.51	Denial of Service, Possible remote code execution	High

2.4 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.

2.5 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.

2.6 Mitigation

GENESIS64 version 10.6 and later is not vulnerable to this exploit. 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.
- 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.
- Do not click web links or open unsolicited attachments in e-mail messages.
- Install the patch:

ICONICS Software Version	Reference ID	Update / File(s) needed	File Version
10.51	15184	10.51 Hot Fix Pack 1	N/A

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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) website. 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 Date: May 2011

3.2 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.

3.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	Severity Rating
GENESIS64, Hyper Historian	All versions up to and including 10.51	Directory Transversal	Medium

3.4 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.

3.5 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).

3.6 Mitigation

GENESIS64 version 10.6 and later is not vulnerable to this exploit. 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.
- 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.
- Do not click web links or open unsolicited attachments in e-mail messages.
- Install the patch.

ICONICS Software Version	Reference ID	Update / File(s) needed	File Version
10.51	15533	10.51 Hot Fix Pack 1	N/A

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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) website. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

4 GenBroker Out-of-Bounds (ICS-CERT Advisory ICSA-20-170-03)

4.1 Date: June 2020

4.2 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 website, http://iconics.com/cert.

4.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GenBroker64 contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.96	Out of Bounds Write, Possible remote code execution	8.1	787 - Out-of-bounds Write	CVE-2020-12007

4.4 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.

4.5 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.

4.6 Mitigation

ICONICS Suite version 10.96.1 and later is not vulnerable to this exploit. 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 Software Version	Reference ID	Update / File(s) needed	File Version / Date Created
10.96	74209	10.96 Critical Fixes Rollup 1	N/A
10.95.5	74379	GenBroker64.exe	10.95.207.0 – 5/7/2020
10.95.2	74378	GenBroker64.exe	10.95.200.0 – 3/27/2020

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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) website. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

5 FWX Server Faulty String Deserialization (ICS-CERT Advisory ICSA-20-170-03)

5.1 Date: June 2020

5.2 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://iconics.com/cert.

5.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
Platform Services contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.96	Denial of Service	7.5	502 - Deserialization of Untrusted Data	CVE-2020-12009

5.4 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.

5.5 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.

5.6 Mitigation

ICONICS Suite version 10.96.1 and later is not vulnerable to this exploit. 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 Software Version	Reference ID	Update / File(s) Needed	File Version – Date Created
10.96	74206	10.96 Critical Fixes Rollup 1	N/A
10.95.5	74388	FwxAsyncCore.dll	10.95.207.0 – 5/7/2020
10.95.2	74387	FwxAsyncCore.dll	10.95.200.0 – 3/27/2020

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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) website. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

6 Security not enforced on Project Files (ICS-CERT Advisory ICSA-20-170-03)

6.1 Date: June 2020

6.2 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 website, http://iconics.com/cert.

6.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
Workbench contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.96	Possible Remote Code Execution	7.5	502 - Deserialization of Untrusted Data	CVE-2020-12011

6.4 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.

6.5 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.

6.6 Mitigation

ICONICS Suite version 10.96.1 and later is not vulnerable to this exploit. 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 Software Version	Reference ID	Update / File(s) Needed	File Version – Date Created
10.96	74154	10.96 Critical Fixes Rollup 1	N/A
10.95.5	74391	IcoWorkbenchPackAndGo.dll	10.95.207.00 – 5/7/2020
10.95.2	74390	IcoWorkbenchPackAndGo.dll	10.95.200.00 – 3/27/2020

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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) website. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies.

7 Missing Security on Procedures and Datasets (ICS-CERT Advisory ICSA-20-170-03)

7.1 Date: June 2020

7.2 Issue – Discussion

On January 22, 2020, researcher Ben McBride of Oak Ridge National Laboratory reported a potential security vulnerability in GENESIS64 10.95 which can result in information disclosure if exploited. ICONICS validated the researcher's claim that in GENESIS64 10.95, 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 (10.96).

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 website, http://iconics.com/cert.

7.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
Platform Services contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.95.5	Information Disclosure Possible Execution of Commands, depending on system setup	9.4	94 - Improper Control of Generation of Code	CVE-2020-12013

7.4 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.

7.5 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.

7.6 Mitigation

ICONICS Suite version 10.96.1 and later is not vulnerable to this exploit. 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 (see table below).
- 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 has patches for the following versions:

ICONICS Software Version	Reference ID	Update / File(s) Needed	File Version – Date Created
10.96	74210	10.96 Critical Fixes Rollup 1	N/A
10.95.5	74382	FwxAsyncCore.dll	10.95.207.0 – 5/7/2020
10.95.2	74381	FwxServerCore.dll, FwxAsyncCore.dll	10.95.200.0 – 3/27/2020 10.95.200.0 – 3/27/2020

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

8 FWX Server Deserialization (ICS-CERT Advisory ICSA-20-170-03)

8.1 Date: June 2020

8.2 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 website, http://iconics.com/cert.

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.

8.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
Platform Services contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.96	Possible Remote Code Execution	7.5	502 - Deserialization of Untrusted Data	CVE-2020-12015

8.4 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.

8.5 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.

8.6 Mitigation

ICONICS Suite version 10.96.1 and later is not vulnerable to this exploit. 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 Software Version	Reference ID	Update / File(s) Needed	File Version – Date Created
10.96	74211 74393 74618	10.96 Critical Fixes Rollup 1	N/A
10.95.5	74385 74396 74623	FwxAsyncCore.dll FwxIotJsonEncoderDecoder.dll FwxServerCore.dll GdxPointManager.dll GenBroker64.exe IcoConfigCommon.dll IcoConfigCommonAG.dll IcoConfiguratorCore.dll	10.95.207.0 - 5/7/2020 10.95.207.0 - 5/7/2020 10.95.207.0 - 5/7/2020 10.95.207.0 - 5/7/2020 10.95.207.0 - 5/7/2020 10.95.207.0 - 5/7/2020 10.95.207.0 - 5/7/2020 10.95.207.0 - 5/7/2020

		IcoEaClient.dll	10.95.207.0 - 5/7/2020
		IcoEaConfiguration.dll	10.95.207.0 - 5/7/2020
		IcoEaDefinitions.dll	10.95.207.0 - 5/7/2020
		IcoEaPowershell.dll	10.95.207.0 - 5/7/2020
		IcoGdxClient.dll	10.95.207.0 - 5/7/2020
		IcoGdxDefinitions.dll	10.95.207.0 - 5/7/2020
		IcoHHClient.dll	10.95.207.0 - 5/7/2020
		IcoHHConfiguration.dll	10.95.207.0 - 5/7/2020
		IcoWorkbenchConfiguration.dll	10.95.207.0 - 5/7/2020
		IcoWorkbenchCore.dll	10.95.207.0 - 5/7/2020
		IcoWorkbenchDefinitions.dll	10.95.207.0 - 5/7/2020
		IcoWorkbenchPackAndGo.dll	10.95.207.0 - 5/7/2020
10.95.2	74384 74395 74622	FwxAsyncCore.dll	10.95.200.0 – 3/27/2020
		FwxIotJsonEncoderDecoder.dll	10.95.200.0 – 3/27/2020
		FwxServerCore.dll	10.95.200.0 – 3/27/2020
		GenBroker64.exe	10.95.200.0 – 3/27/2020
		IcoCommon.dll	10.95.200.0 – 3/30/2020
		IcoConfigCommon.dll	10.95.200.0 – 3/27/2020
		IcoConfigCommonAG.dll	10.95.200.0 – 3/27/2020
		IcoConfiguratorCore.dll	10.95.200.0 – 3/27/2020
		IcoEaClient.dll	10.95.200.0 – 3/27/2020
		IcoEaConfiguration.dll	10.95.200.0 – 3/27/2020
		IcoEaDefinitions.dll	10.95.200.0 – 3/27/2020
		IcoEaPowershell.dll	10.95.200.0 – 3/27/2020
		IcoHHClient.dll	10.95.200.0 – 3/27/2020
		IcoHHConfiguration.dll	10.95.200.0 – 3/27/2020
		IcoWorkbenchConfiguration.dll	10.95.200.0 – 3/27/2020
		IcoWorkbenchCore.dll	10.95.200.0 – 3/27/2020
		IcoWorkbenchDefinitions.dll	10.95.200.0 – 3/27/2020
		IcoWorkbenchPackAndGo.dll	10.95.200.0 – 3/27/2020

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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) website. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cyber security with Defense-in-Depth Strategies.

9 OPC UA Framework Uncontrolled Recursion (ICS-CERT Advisory ICSA-21-294-03)

9.1 Date: October 2021

9.2 Issue – Discussion

On May 13, 2021, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published advisory ICSA-21-133-03 on the OPC Foundation's SDK for OPC UA products built with .NET Framework. ICONICS products use this SDK.

OPC Foundation has fixed this vulnerability in OPC UA SDK version 1.4.365.48 (and newer).

ICONICS is working on a set of downloadable patches for this vulnerability that include the solution published by the OPC Foundation. In addition, the steps listed below can be used to mitigate this vulnerability. These patches can be downloaded from the ICONICS Customer Connection portal.

9.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
All ICONICS Suite products (including GENESIS64, Hyper Historian, MobileHMI)	All versions up to and including 10.97.	Denial of Service	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	674 - Uncontrolled Recursion	CVE-2021-27432

9.4 Impact

A successful exploit of this vulnerability can create uncontrolled recursion, which may allow an attacker to trigger a stack overflow, and ultimately, this can in turn crash the affected component.

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.

9.5 Vulnerability

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT:

There is no known exploit code specifically targeting this vulnerability other than 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.

9.6 Mitigation

Version 10.97.1 and later is not vulnerable to this exploit. 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.
- Leverage OPC UA security and certificates to ensure that ICONICS products only connect to trusted OPC UA servers and clients.
- Install the patch:

ICONICS Software Version	Reference ID	Update / File(s) Needed	File Version
10.97	84200	10.97 Critical Fixes Rollup 2	N/A
10.96.2	84258	10.96.2 Critical Fixes Rollup 2	N/A
10.95.5	84838	Opc.Ua.Core.dll	1.03.340.2

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

10 GraphWorX64 AutoCAD Import OOB (ICS-CERT Advisory ICSA-21-294-01)

10.1 Date: October 2021

10.2 Issue – Discussion

In July 2021, Trend Micro identified and reported a vulnerability in the GENESIS64 GraphWorX64 AutoCAD (DWG) file import function. This potential security vulnerability can result in remote code execution, if exploited.

ICONICS validated the researcher's claim that if a specially crafted, malicious AutoCAD DWG file is imported into GraphWorX64, it could make GraphWorX64 susceptible to an out-of-bounds write attack as well as an out-of-bounds read attack. The specific flaw exists in the parsing of DWG files that exists in a third-party library used by the ICONICS products. The issue results from the lack of proper validation of user-supplied data. User interaction is required to exploit this vulnerability. The user must specifically request GraphWorX64 to import the malicious file.

ICONICS is addressing this issue by:

- Providing a set of patches to currently released versions of GraphWorX64 that will add a warning message, advising the user to be sure all DWG files being imported are known to come from a trusted source.
- Providing a version of GraphWorX64 in the upcoming version 10.97.1 release that will no longer be susceptible to this security vulnerability issue.

The patches will be included in upcoming Critical Fixes Rollup releases which can be downloaded from the ICONICS Customer Connection Portal.

10.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GENESIS64 (GraphWorX64)	All versions up to and including 10.97	Possible Remote Code Execution	7.8	787 - Out-of-bounds Write	CVE-2021-40156, CVE-2021-40155

10.4 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.

10.5 Vulnerability

Exploitation of this file import issue requires creation of a specially crafted AutoCAD DWG file and requires user interaction.

EXPLOITABILITY:
This vulnerability is remotely exploitable but does require user interaction.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting this vulnerability other than 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 AutoCAD DWG file format, knowledge on how AutoDesk's libraries parse DWG files, and being able to craft a special DWG file that takes advantage of a flaw in the input checking.

10.6 Mitigation

Version 10.97.1 and later is not vulnerable to this exploit. 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.
- When importing any AutoCad DWG file, make sure it is known to come from a trusted source
- Install the applicable Critical Fixes Rollup, if available:

ICONICS Software Version	Reference ID	Update / File(s) Needed
10.97	85286	10.97 Critical Fixes Rollup 2
10.96.2	85287	10.96.2 Critical Fixes Rollup 3 (Release pending)
10.96.1	85323	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	85322	10.96 Critical Fixes Rollup 6 (Release pending)

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

11 Cross-Site Scripting (ICS-CERT Advisory ICSA-22-020-01)

11.1 Date: January 2022

11.2 Issue – Discussion

In January 2022, ICONICS reported a cross-site scripting security vulnerability exists in the MobileHMI product. This security vulnerability can make it possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing an attacker to view or alter user records, and to perform transactions as that user.

The issue results from the lack of proper validation checking on user input and external data when it is used to render a page to the client.

ICONICS is addressing this issue by providing a patch to the currently released version of ICONICS Suite that will add additional validation checking on inputs and external data. This patch will be included in upcoming Critical Fixes Rollup releases which can be downloaded from the ICONICS Customer Connection Portal.

11.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GENESIS64 (WebHMI), MobileHMI	All versions up to and including 10.96.2	Unauthorized access to information	4.2 (AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/RL:O)	79 - Improper Neutralization of Input During Web Page Generation	CVE-2022-23127

11.4 Impact

A successful exploit of this vulnerability can potentially result in unauthorized access to information.

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.

11.5 Vulnerability

EXPLOITABILITY:
Exploitation of this issue requires the attacker to trick the authenticated user to follow an URL pointing to the vulnerable component. Then he could be able to steal the session cookie from the presentation layer and use it to steal the victim's identity.

EXISTENCE OF EXPLOIT:

There is no known exploit code specifically targeting this vulnerability.

DIFFICULTY:
A successful attack requires the attacker to invest measurable amount of effort in preparation against the deployed system before a successful attack can be expected. The attacker must know the presentation layer of deployed application to exploit. The presentation layer has no direct access to the API, so the attacker does not have control over what information is obtained.

11.6 Mitigation

Version 10.97 and later is not vulnerable to this exploit. 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 applicable Critical Fixes Rollup, if available:

ICONICS Suite Version	Reference ID	Updates / File(s) Needed
10.96.2	81168	10.96.2 Critical Fixes Rollup 1
10.96.1	81110	10.96.1 Critical Fixes Rollup 2

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

12 Incomplete List of Disallowed Inputs (ICS-CERT Advisory ICSA-22-020-01)

12.1 Date: January 2022

12.2 Issue – Discussion

This vulnerability can allow an attacker to bypass the GENESIS64 Security system if they open a communication channel to the WebSocket endpoint (port 80 or 443) of the FrameWorX Server and modify some of the parameters that are sent during the handshake. The issue results from the lack of proper validation checking during the handshake process when a client application attempts to open a communications channel.

ICONICS has addressed this issue by providing a patch for the currently released version of ICONICS Suite that enhances the checking in the Web Socket endpoint in FrameWorX Server. Additional validation checking was added on the parameters during the handshake process and connections with unexpected values being refused. This patch is included in recent Critical Fixes Rollup releases which can be downloaded from the ICONICS Customer Connection Portal.

12.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
Platform Services contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions from 10.95.3 to 10.97	Unrestricted access to GENESIS64 functionality	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	184 - Incomplete List of Disallowed Inputs	CVE-2022-23128

12.4 Impact

A successful exploit of this vulnerability can potentially result in unrestricted access to GENESIS64 functionality.

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.

12.5 Vulnerability

EXPLOITABILITY:
Exploitation of this issue requires the attacker to modify the handshake parameters when setting up a WebSocket communications channel. They would either have to implement the communication protocol of FrameWorX Server, or possibly find a way to use the ICONICS binaries to do it with modified parameters.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting this vulnerability.

DIFFICULTY:
An attacker would need a high skill level to be able to exploit this vulnerability. It requires attaining knowledge of the protocol FrameWorX Server uses to set up WebSocket communications.

12.6 Mitigation

Version 10.97.1 and later is not vulnerable to this exploit.

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 applicable Critical Fixes Rollup, if available:

The following Critical Fix Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97	86183	10.97 Critical Fixes Rollup 2
10.96.2	86182	10.96.2 Critical Fixes Rollup 3
10.96.1	86181	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	86180	10.96 Critical Fixes Rollup 6 (Release pending)

Another mitigation that can be performed on a system with this vulnerability (one that does not have a software patch that addresses the vulnerability) is to switch to WCF communications and then disable the WebSocket protocol in FrameWorX Server. To disable the WebSocket protocol in FrameWorX Server, one must simply edit the file 'FwxServer.Network.config' and set the WebSocketsTransport element to false.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

13 Plaintext Storage of Password (ICS-CERT Advisory ICSA-22-020-01)

13.1 Date: January 2022

13.2 Issue – Discussion

The GENESIS64 Workbench export to CSV function may expose a password in plain text when it is used to export the GridWorX Server configuration. The issue is a result of a coding error in Workbench.

ICONICS has addressed this issue by providing a patch for the currently released version of GENESIS64 that always encrypts such passwords. This patch is included in recent Critical Fixes Rollup releases which can be downloaded from the ICONICS Customer Connection Portal.

13.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
Workbench (Databases/GridWorX Provider) contained in all ICONICS Suite products	All versions from 10.90 to 10.97	Unauthorized access to information	7.7 (AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H)	256 - Plaintext Storage of a Password	CVE-2022-23129

13.4 Impact

A successful exploit of this vulnerability can result in unauthorized access to the SQL Server database that contains the GridWorX Server's configuration information.

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.

13.5 Vulnerability

EXPLOITABILITY:
Exploitation of this issue requires the attacker to use Workbench to export the configuration of GridWorX Server to a CSV file.

EXISTENCE OF EXPLOIT:
Not Applicable.

DIFFICULTY:
An attacker with a relatively low skill level would be able to exploit this vulnerability.

13.6 Mitigation

Version 10.97.1 and later is not vulnerable to this exploit. 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 applicable Critical Fixes Rollup, if available:

The following Critical Fix Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97	82376	10.97 Critical Fixes Rollup 1
10.96.2	82402	10.96.2 Critical Fixes Rollup 1
10.96.1	82400	10.96.1 Critical Fixes Rollup 3
10.96	82399	10.96 Critical Fixes Rollup 5

A mitigation that can be performed on a system with this vulnerability (a system that does not have a software patch that addresses the vulnerability) is:

1. Once the file is exported, the user deletes the password from the CSV file before distributing it. The user would also need to immediately delete the task from the Workbench tasks. Otherwise, the file will be still stored on the file system.
2. The user can remove the password before performing the export. To do this, the user needs to open the connection configuration in Workbench (under Databases > SQL Connections), remove the password from the connection string, and apply the changes. The configuration can now be exported safely. Once the export is complete, the user can edit the connection configuration again and put back the password. Note, removing the password in this way may make the GridWorX point manager data temporarily inaccessible.
3. The system administrator can disable the GridWorX provider from the security for users who do not need access.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

14 SQL Query Engine Buffer Over-read (ICS-CERT Advisory ICSA-22-020-01)

14.1 Date: January 2022

14.2 Issue – Discussion

This security vulnerability made it possible to execute a series of SQL commands in a GENESIS64 system that could cause a crash of the SQL Query Engine and ultimately could result in a disabling of SQL Server. The issue is a result of a coding error in the SQL Query Engine memory allocation code.

ICONICS has addressed this issue by providing a patch for the currently released version of ICONICS Suite that correctly handles memory allocation. This patch is included in recent Critical Fixes Rollup releases which can be downloaded from the ICONICS Customer Connection Portal.

14.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
All ICONICS Suite (including GENESIS64, Hyper Historian, MobileHMI)	All versions up to and including 10.97	Denial of Service	5.9 (AV:A/AC:H/PR:H/UI:R/S:C/C:N/I:L/A:H)	126 – Buffer Overread	CVE-2022-23130

14.4 Impact

A successful exploit of this vulnerability can potentially result in a crash of the SQL Query Engine and ultimately could result in a disabling of SQL Server.

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.

14.5 Vulnerability

EXPLOITABILITY:
Exploitation of this issue requires the attacker to know credentials to the SQL Server where the SQL Query Engine is installed, plus the attacker needs to know a command that has to be executed.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting this vulnerability.

DIFFICULTY:
Exploitation of this issue requires the attacker to know credentials to the SQL Server where the SQL Query Engine is installed, plus the attacker needs to know a command that has to be executed. An attacker with a moderate skill level would be able to exploit this vulnerability.

14.6 Mitigation

Version 10.97.1 and later is not vulnerable to this exploit. 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 applicable Critical Fixes Rollup, if available:

The following Critical Fix Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97	85753	10.97 Critical Fixes Rollup 2
10.96.2	85752	10.96.2 Critical Fixes Rollup 3 (Release pending)
10.96.1	85751	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	85750	10.96 Critical Fixes Rollup 6 (Release pending)

A mitigation that can be performed on a system with this vulnerability (a system that does not have a software patch that addresses the vulnerability) is to implement strict SQL Server security so that users have only the minimum rights necessary.

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

15 MobileHMI Path Traversal (ICS-CERT Advisory ICSA-22-202-04)

15.1 Date: July 2022

15.2 Issue – Discussion

On April 15, 2022, researchers Chris Anastasio and Steven Seeley of Incite working with Trend Micro Zero Day Initiative, reported a file path traversal vulnerability in the MobileHMI product. Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of a restricted directory on the MobileHMI AnyGlass server.

ICONICS validated the researcher's claim and has addressed this issue in version 10.97.2 of ICONICS Suite.

15.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
MobileHMI, HTML5, WebHMI, and IoTWorX Visualizer	Versions 10.97 and 10.97.1	Information Disclosure	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	22 - Improper Limitation of a Pathname to a Restricted Directory	CVE-2022-29834

15.4 Impact

The impact of a successful exploit of this vulnerability is that an attacker can leverage a path traversal vulnerability in the system to step out of the root directory, allowing them to access other parts of the file system to view restricted files and gather more information required to further compromise the system.

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.

15.5 Vulnerability

EXPLOITABILITY:
Exploitation of this issue requires the attacker to access a certain endpoint in MobileHMI which can give them unauthorized access to certain files.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting this vulnerability.

DIFFICULTY:
An attacker with a moderate skill level may be able to exploit this vulnerability.

15.6 Mitigation

Version 10.97.2 and later is not vulnerable to this exploit. 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.
- Use the 10.97.2 or later version of the ICONICS products.
- Install the applicable Critical Fixes Rollup, if available.

The following Critical Fix Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97.1	89588	10.97.1 Critical Fixes Rollup 3
10.97	89589	10.97 Critical Fixes Rollup 4 (Release pending)

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

16 GraphWorX64 Deserialization (ICS-CERT Advisory ICSA-22-202-04)

16.1 Date: July 2022

16.2 Issue – Discussion

On April 15, 2022, researcher Alex Birmberg of Zymo Security working with Trend Micro Zero Day Initiative, reported a security vulnerability in GraphWorX64 with deserialization of untrusted data which can result in remote code execution if exploited. Note, this security vulnerability was later reported by Chris Anastasio and Steven Seely of Incite, and others, at the Pwn2Own 2022 conference. And a related security vulnerability was later reported by Noam Moshe of Claroty Research working with Trend Micro Zero Day Initiative. ICONICS validated the researchers' claim and has addressed this issue in version 10.97.2 of ICONICS Suite.

16.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVEs
GraphWorX64	All versions up to and including 10.97.1	Possible Remote Code Execution	7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	502 – Deserialization of Untrusted Data	CVE-2022-33315 CVE-2022-33316 CVE-2022-33320

16.4 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.

16.5 Vulnerability

Exploitation of this deserialization issue requires creation of a specially crafted GraphWorX64 file and requires user interaction. The GraphWorX64 file types affected by this vulnerability include the standard display files (.gdfx), template files (.tdfx), and trend, alarm, grid, and schedule configuration files (.twxx, .awxx, .gdxx, and .schx files).

EXPLOITABILITY:
This vulnerability is remotely exploitable but does require user interaction.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting this vulnerability other than 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 GraphWorX64 file format and being able to craft a special GraphWorX64 file that takes advantage of a flaw in the deserialization.

16.6 Mitigation

Version 10.97.2 and later is not vulnerable to this exploit. 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.
- Use only GraphWorX files that are known to come from a trusted source.
- Use the 10.97.2 or later version of the ICONICS products.
- If using an earlier version, install the applicable Critical Fixes Rollup, if available.

The following Critical Fix Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97.1	90086 90087 90088 90089 90090 90091 90314	10.97 Critical Fixes Rollup 3
10.97	TBD	10.97 Critical Fixes Rollup 4 (Release pending)
10.96.2	TBD	10.96.2 Critical Fixes Rollup 3 (Release pending)
10.96.1	TBD	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	TBD	10.96 Critical Fixes Rollup 6 (Release pending)

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

17 GraphWorX64 Scripting (ICS-CERT Advisory ICSA-22-202-04)

17.1 Date: July 2022

17.2 Issue – Discussion

On April 20, 2022, researcher Ben McBride working with Trend Micro Zero Day Initiative, reported a security vulnerability with GraphWorX64's scripting environment. GraphWorX64 scripting, based on JScript and .NET, stores its script code in the GraphWorX64 project files. The project files can be directly edited, and as a result, this poses a security risk. If an attacker has access to the project files or convinces the user to load a compromised project file, it can result in remote code execution. ICONICS validated the researchers' claim and has taken steps to mitigate this issue in version 10.97.2 of ICONICS Suite, and in 10.97.1 Critical Fixes Rollup 3.

17.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GraohWorX64	All versions up to and including 10.97.1	Possible remote code execution	7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	829 – Inclusion of Functionality from Untrusted Control Sphere	CVE-2022-33317

17.4 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.

17.5 Vulnerability

Exploitation of this security issue requires creation of a specially crafted GraphWorX64 project file (.gdfx, .tdfx, .twxx, .awxx, .gdxx, or .schx) file and requires user interaction.

EXPLOITABILITY:
This vulnerability is remotely exploitable but does require user interaction.

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

DIFFICULTY:
An attacker would need a low/medium skill level to be able to exploit this vulnerability. It requires some basic knowledge of the JScript.NET programming language (and .NET in general), and some basic knowledge of how JScript.NET is used in GraphWorX64.

17.6 Mitigation

ICONICS has added an option in v10.97.2 to allow disabling of scripting in GraphWorX64. 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.
- Disable GraphWorX64 scripting if it is not needed nor being used. (Note, the option to disable scripting is available in v10.97.2 and later).
- Use only GraphWorX project files (.gdfx, .tdfx, .twxx, .awxx, .gdxx, and .schx files) that are known to come from a trusted source.
- Install the applicable Critical Fixes Rollup, if available, and disable GraphWorX64 scripting if it is not needed nor being used.

The following Critical Fix Rollups include the option to disable GraphWorX64 scripting:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97.1	90093	10.97.1 Critical Fixes Rollup 3
10.97	TBD	10.97 Critical Fixes Rollup 4 (Release pending)
10.96.2	TBD	10.96.2 Critical Fixes Rollup 3 (Release pending)
10.96.1	TBD	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	TBD	10.96 Critical Fixes Rollup 6 (Release pending)

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

18 GenBroker Deserialization of Untrusted Data (ICS-CERT Advisory ICSA-22-202-04)

18.1 Date: July 2022

18.2 Issue – Discussion

On April 20, 2022, researcher Axel '0vercl0k' Souchet working with Trend Micro Zero Day Initiative, reported a deserialization issue in GenBroker64 where if exploited, can result in remote code execution. ICONICS validated the researchers' claim and has addressed this issue in version 10.97.2 of ICONICS Suite.

18.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GenBroker64 contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.97.1	Possible remote code execution	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	502 - Deserialization of Untrusted Data	CVE-2022-33318

18.4 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.

18.5 Vulnerability

Exploitation of this 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 than 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 determining the deserialization issue that GenBroker is vulnerable to and requires crafting of a special communications packet to take advantage of it.

18.6 Mitigation

Version 10.97.2 and later is not vulnerable to this exploit. 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.
- Use the 10.97.2 or later version of the ICONICS products.
- If using an earlier version, install the applicable Critical Fixes Rollup, if available.

The following Critical Fix Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97.1	89733	10.97 Critical Fixes Rollup 3
10.97	90459	10.97 Critical Fixes Rollup 4 (Release pending)
10.96.2	90460	10.96.2 Critical Fixes Rollup 3 (Release pending)
10.96.1	90461	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	90462	10.96 Critical Fixes Rollup 6 (Release pending)

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

19 GenBroker Out-of-Bounds Read (ICS-CERT Advisory ICSA-22-202-04)

19.1 Date: July 2022

19.2 Issue – Discussion

On May 25, 2022, researcher Axel '0vercl0k' Souchet, working with Trend Micro Zero Day Initiative, reported an out-of-bounds read issue in GenBroker64 where if exploited, can result in information disclosure or potentially a crash of GenBroker64 and a denial of service issue. ICONICS validated the researchers' claim and has addressed this issue in version 10.97.2 of ICONICS Suite.

19.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GenBroker64 contained in all ICONICS Suite products, including: • GENESIS64 • Hyper Historian • AnalytiX • MobileHMI	All versions up to and including 10.97.1	Information Disclosure, Possible denial of service	8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H)	125 - Out-of-bounds Read	CVE-2022-33319

19.4 Impact

A successful exploit of this vulnerability can potentially result in information disclosure or a crash of GenBroker64 and consequently, a 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.

19.5 Vulnerability

Exploitation of this GenBroker64 vulnerability requires creation of a specially crafted communication packet which must be sent to GenBroker64'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 than 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 determining the out-of-bounds read issue that GenBroker64 is vulnerable to and requires crafting of a special communications packet to take advantage of it.

19.6 Mitigation

Version 10.97.2 and later is not vulnerable to this exploit. 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.
- Use the 10.97.2 or later version of the ICONICS products.
- If using an earlier version, install the applicable Critical Fixes Rollup, if available.

The following Critical Fix Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97.1	90452	10.97 Critical Fixes Rollup 3
10.97	90453	10.97 Critical Fixes Rollup 4 (Release pending)
10.96.2	90454	10.96.2 Critical Fixes Rollup 3 (Release pending)
10.96.1	90455	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	90456	10.96 Critical Fixes Rollup 6 (Release pending)

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

20 Path Traversal in Workbench (ICS-CERT Advisory ICSA-22-347-01)

20.1 Date: December 2022

20.2 Issue – Discussion

On July 22, 2022, researcher Noam Moshe at Claroty Research with Trend Micro Zero Day Initiative, reported a path traversal vulnerability in the GENESIS64 Workbench Pack&Go function. Successful exploitation could allow an attacker to force Workbench to write an arbitrary file.

ICONICS validated the researcher's claim and has addressed this issue in version 10.97.2 Critical Fixes Rollup 1 of the ICONICS Suite.

20.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS	CWE	CVE
Workbench contained in all ICONICS Suite products	Versions 10.96 through 10.97.2	File tampering	6.3 (AV:L/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N)	22 - Improper Limitation of a Pathname to a Restricted Directory	CVE-2022-40264

20.4 Impact

The impact of a successful exploit of this vulnerability is that an attacker can create, tamper with or destroy arbitrary files.

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.

20.5 Vulnerability

EXPLOITABILITY:
Exploitation of this issue requires the attacker to understand the Workbench Pack&Go package file format, to create a specially crafted Pack&Go package, and to use social engineering to get the specially crafted package onto a system.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting this vulnerability.

DIFFICULTY:
An attacker with a low skill level may be able to exploit this vulnerability.

20.6 Mitigation

Version 10.97.2 Critical Fixes Rollup 1 and later is not vulnerable to this exploit. 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.
- Use the 10.97.2 Critical Fixes Rollup 1 or later version of the ICONICS products.
- Install the applicable Critical Fixes Rollup, if available.
- For systems that do not contain the patch/fix:
    - Only unpack files coming from trusted sources
    - Protect and encrypt Pack&Go packages with a password to prevent modifications by untrustworthy users
    - Do not unpack a Pack&Go package file if it is using a relative path (Note, this would show up in the Workbench UI)

The following Critical Fixes Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
10.97.2	91163	10.97.2 Critical Fixes Rollup 1
10.97.1	91162	10.97.1 Critical Fixes Rollup 4 (Release pending)
10.97	91161	10.97 Critical Fixes Rollup 4 (Release pending)
10.96.2	91160	10.96 Critical Fixes Rollup 3 (Release pending)
10.96.1	91159	10.96.1 Critical Fixes Rollup 4 (Release pending)
10.96	91158	10.96 Critical Fixes Rollup 6 (Release pending)

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

21 BACnet/SC Buffer Overrun

21.1 Date: December 2022

21.2 Issue – Discussion

On November 1, 2022, openssl.org published a security advisory on OpenSSL where a buffer overrun can be triggered in X.509 certificate verification. An attacker taking advantage of this vulnerability may be able to cause a crash (causing a denial of service) or potentially remote code execution.

The GENESIS64 BACnet/SC feature included in the v10.97.2 release in a "Beta" version, is susceptible to this vulnerability. As a result, the BACnet/SC feature in version v10.97.2 should only be used in a test environment. Note, GENESIS64 10.97.2 systems that are not using the BACnet/SC feature are not susceptible to this issue, nor are any previous versions of GENESIS64 up to and including version 10.97.1.

ICONICS has addressed this issue in the Version 10.97.2 Critical Fixes Rollup 1 release.

21.3 Products Affected

The following table identifies ICONICS products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS	CWE	CVE
GENESIS64 BACnet/SC feature	Version 10.97.2	Denial of Service, Potential Remote Code Execution	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	120 - Buffer Copy without Checking Size of Input	CVE-2022-3602, CVE-2022-3786

21.4 Impact

The impact of a successful exploit of this vulnerability is that an attacker can cause a denial of service and potentially 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.

21.5 Vulnerability

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting this vulnerability.

DIFFICULTY:
An attacker would need a high skill level to be able to exploit this vulnerability.

21.6 Mitigation

Version 10.97.2 Critical Fixes Rollup 1 and later is not vulnerable to this exploit. ICONICS recommends that users of its products take the following mitigation steps:

- For systems that do not contain the patch/fix:
  - Do not use the BACnet/SC feature on a production system.
- 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.
- Use the 10.97.2 Critical Fixes Rollup 1 or later version of the ICONICS products.
- Install the applicable Critical Fixes Rollup, if available.

The following Critical Fixes Rollup releases contain the fix for this vulnerability:

ICONICS Suite Version	Reference ID	Update / File(s) Needed
v10.97.2	92026	10.97.2 Critical Fixes Rollup 1

ICONICS provides information and useful links related to its security updates, as well as the patch described above, at its website at http://iconics.com/cert. 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.

Appendix A – Other Security Topics

WHITEPAPER ON ICONICS SUITE SECURITY
VULNERABILITIES – OTHER TOPICS

100 Foxborough Blvd., Foxborough, MA 02035

1 ICONICS Response to Microsoft Windows DCOM Hardening

1.1 Date: March 2022

1.2 Issue – Discussion

To address a security vulnerability (CVE-2021-26414), Microsoft is hardening the Distributed Component Model (DCOM) on its Windows operating systems. The next stage of the DCOM hardening will occur on June 14, 2022, where hardening changes will be enabled by default. Currently, hardening changes are disabled by default but can be enabled via registry key.

DCOM has traditionally been the communication method used to communicate with OPC Classic servers across the network. ICONICS software can leverage DCOM communication, but by default and by best practice, most ICONICS software (both 64-bit and 32-bit) uses GenBroker communication via TCP/IP to tunnel to remote OPC Classic servers. This means that most ICONICS applications will not be affected by this hardening of DCOM security.

The following situations will NOT be affected by DCOM hardening:

- ICONICS client communicating with an OPC Classic server on the same machine.
- ICONICS client communicating with an OPC Classic server on a remote machine when configured to use GenBroker and the "OPC over TCP/IP" or "OPC over SOAP/XML" channels.
- ICONICS client communicating with an OPC UA server, database, BACnet device, SNMP device, or other devices.

The situations below are likely to be affected by the upcoming DCOM hardening and may require configuration changes:

- ICONICS client communicating with an OPC Classic server on a remote machine when configured to use the "OPC Direct" channel.
- ICONICS client communicating with an OPC Classic server on a remote machine when configured to use GenBroker and the "OPC over DCOM" channel.
- Custom scripts (including scripts running inside ScriptWorX32, ScriptWorX2010, ScriptWorX64, GraphWorX32, or GraphWorX64) that use OPC Foundation libraries or other non-ICONICS libraries to communicate with an OPC Classic server on a remote machine.
- Third-party client communicating with an ICONICS OPC Classic server on a remote machine without using a tunnel.

If your application contains one of the affected situations, ICONICS recommends implementing one or more of the following changes to prepare for DCOM hardening:

- Install and run GenBroker Server on the machine with the remote OPC Classic server.
- Use the GenBroker64 Settings in Workbench or the GenBroker Configurator to configure the "OPC over TCP/IP" channel for use with your remote OPC Classic server for ICONICS clients.
- Modify custom scripts to use ICONICS libraries and functions (such as "g.OPC" in ScriptWorX2010 or ScriptWorX64) that can take advantage of GenBroker communication.

100 Foxborough Blvd., Foxborough, MA 02035

- Upgrade OPC Classic servers to OPC UA servers if the client supports it. (Note: ICONICS clients from the 32-bit generation, such as GENESIS32 and BizViz, do not support OPC UA.)
- Use a tunneler for third-party OPC Classic clients.
- (Not recommended) Disable the Microsoft advanced security measures with a registry key. Note, this solution will not function after March 14, 2023, and may leave your system open to a security breach via DCOM.

To account for the DCOM hardening, ICONICS will start labeling the "OPC Direct" and "OPC over DCOM" channels as "obsolete" in version 10.97.2 and discourage the use of these channels. These will be completely unavailable in future versions.

For more information about Microsoft's DCOM hardening, see this Microsoft support article.

For additional questions about ICONICS' response to DCOM hardening and configuration changes that may be required, contact your local technical support department.

100 Foxborough Blvd., Foxborough, MA 02035