WHITEPAPER ON SECURITY VULNERABILITIES

2016 V9

MARCH 2016

An ICONICS Whitepaper

CONTENTS

100 Foxborough Blvd., Foxboro, 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 vulnerabilities in ICONICS' GENESIS32™ and GENESIS64™ products (ICS-Alert-11-080-02).
3	SafeNet Licensing Driver in the GENESIS32, GENESIS64 and BizViz products, (ICS-CERT Advisory 11-108-01))
4	WebHMI buffer overflow vulnerability in the GENESIS32 and BizViz products (ICS-CERT Advisory 11-131-01)
5	Security Login vulnerability in the GENESIS32 and BizViz products (ICS-CERT Advisory 11-182-02)
6	SetTrustedZone Policy vulnerability in the GENESIS32 and BizViz products (ICS-CERT Advisory 11-182-01)
7	GENESIS32 (ScriptWorX32, GraphWorX32, and AlarmWorX32 Write Access Violation, and TrendWorX32 memory corruption (ICS-CERT Advisory 11-273-01)
8	Authentication Bypass vulnerability in the GENESIS32 and BizViz products (ICS-CERT Advisory 12-212-01)
9	Insecure ActiveX Control in the GENESIS32 product (ICS-CERT Advisory 14-051-01)

ICONICS GENESIS32™, GENESIS64™ and BizViz™ 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/waste water, utilities (including renewable) and others. The products are used globally with an estimated distribution of 55% in the USA, 40% in Europe, and 5% in Asia.

ICONICS recommends that users of its Version 8 and Version 9 products (BizViz™, GENESIS32™, and WebHMI) 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.

Users planning to use the Internet or other third party networks as an integral part of the control and SCADA system should consider using the ICONICS V10 products (GENESIS64™, Hyper Historian, AnalytiX, and MobileHMI).

100 Foxborough Blvd., Foxborough, MA 02035

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

2.1 Issue – Discussion

On March 21, 2011, US-CERT issued a series of alerts regarding possibly vulnerabilities in four companies' SCADA software products, based upon the work of an independent researcher. One alert, ICS-Alert-11-080-02, discussed possible vulnerabilities in 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, http://www.iconics.com/certs, and additional patches as described herein will be available shortly at the same Web site.

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

2.2 Products Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32 and BizViz V8.05 – GenBroker	Windows 2000, Windows XP, Windows Server 2003	Denial of Service	Medium
GENESIS32 and BizViz V9.0 – GenBroker	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Denial of Service	Medium
GENESIS32 and BizViz V9.1 and V9.2 – GenBroker	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Denial of Service	Medium
GENESIS64 V10.51 – GenBroker	Windows 7, Windows Server 2003, Windows Server 2008	Denial of Service	Medium

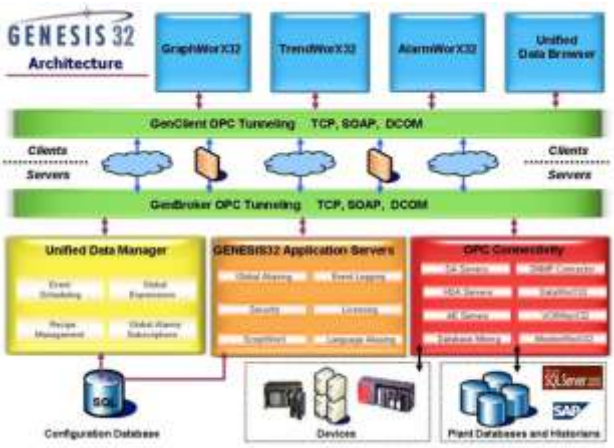
2.3 Impact

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.

A description of how this service is utilized in the GENESIS32 system architecture is described below:



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. 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.

If there is a delay in installing the above patch, we also remind system administrators that they can select optional ports for the GenBroker service using a feature supplied with the product. This feature is demonstrated below in the GenBroker configurator screen shot.

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 Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32 and BizViz V8.05 –Licensing	Windows 2000, Windows XP, Windows Server 2003	Directory Transversal	Medium
GENESIS32 and BizViz V9.1 and V9.2 – Licensing	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Directory Transversal	Medium
GENESIS64 V10.51 – Licensing	Windows 7, Windows Server 2003, Windows Server 2008	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 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.

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 WebHMI (ICS-CERT Advisory 11-131-01)

4.1 Issue – Discussion

On April 28, 2011, Scott Bell and Blair Strang of Security-Assessment.com issued an advisory regarding a potential buffer overflow vulnerability in the ICONICS WebHMI product.

ICONICS validated the researcher's claims for the 9.21 version of WebHMI which is part of the GENESIS32 and BizViz V9.21 product families. ICONICS has released downloadable patches, as well as steps, listed below, to further mitigate the vulnerabilities. The patches for 9.21 can be downloaded at the ICONICS Support Web site, http://www.iconics.com/certs, and additional patches as described herein will be available shortly at the same Web site.

4.2 Products Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32 and BizViz V9.0, V9.1 and V9.2 – WebHMI	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Denial of Service	Medium

4.3 Impact

A successful exploit of the WebHMI buffer overflow 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.

4.4 Vulnerability

The discovered vulnerability exists in the GenVersion.dll: a component that is present in several of the GENESIS32 and BizViz WebHMI CAB files and is used to check versioning. Exploitation of this vulnerability requires a user with the ActiveX control installed to visit a page containing specially crafted JavaScript. By passing a specially crafted string to the "SetActiveXGUID" method, it is possible to overflow a static buffer and execute arbitrary code on the user's machine with the privileges of the logged on user.

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 this vulnerability. The Denial of Service vulnerability exploit would require development of a malicious application that has access to a WebHMI Server machine, and an understanding of the interface to the GenVersion dynamic linked library (dll). The malicious application would need to pass a specially crafted string to a certain method of this dll.

4.5 Mitigation

ICONICS is releasing updated versions of WebHMI CAB files for GENESIS32™ and BizViz™ versions 9.01, 9.13 9.21 that protects against this potential buffer overflow. This issue is addressed in GENESIS32 and BizViz version 9.22 as well.

ICONICS recommends that users of GENESIS32™ and BizViz™ 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.
- Do not use WebHMI server machines as Internet-facing Web clients.
- 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 Security Login (ICS-CERT Advisory 11-182-02)

5.1 Issue – Discussion

On May 10, 2011, researchers Billy Rios and Terry McCorkle reported a possible security related vulnerability in the GENESIS32™ product. This vulnerability is a potential crash in the Security Login controls used by GENESIS32 due to a buffer overrun.

ICONICS validated the researcher's claims for the 9.21 version of GENESIS32 and worked with the researchers on patch validation. ICONICS has released a downloadable patch, as well as steps listed below, to further mitigate this vulnerability. This patch for 9.21 can be downloaded at the ICONICS Support Web site, http://www.iconics.com/certs, and additional patches as described herein will be available shortly at the same web site. This issue is addressed in GENESIS32 version 9.22 as well.

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

5.2 Products Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32™ and BizViz V8.05, V9.0, V9.1 and V9.2 – Login, Login ActiveX, and Security Server	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Denial of Service Possible code execution	High

5.3 Impact

A successful exploit of the Security Login vulnerability could cause a buffer overrun leading to a crash (denial of service), and potentially to 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.

5.4 Vulnerability

The discovered vulnerability exists in the security related components of GENESIS32 and BizViz. Exploitation of the Security Login vulnerability requires creation of a specially crafted password that contains executable code and the hooks to execute the code, in a password that exceeds a certain length.

EXPLOITABILITY:
These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting these vulnerabilities.

DIFFICULTY:
An attacker with a relatively low skill level can create the Denial of Service whereas it would require at least an advanced skill level to perform a code-execution exploit of the Security Login vulnerability. The Security Code-Execution vulnerability exploit would require development of a malicious application that has access to a GENESIS32 or BizViz system, an understanding of the interface to the Login.exe, LoginActiveX.dll, or the SecAutoUtil.dll, and the skills to create a specially crafted password.

5.5 Mitigation

ICONICS is releasing patches for the GENESIS32™ and BizViz™ security files for versions 8.05, 9.01, 9.13 9.21 that protects against the buffer overrun and potential crash.

ICONICS recommends that users of GENESIS32™ and BizViz™ 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 patches.

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 SetTrustedZone Policy (ICS-CERT Advisory 11-182-01)

6.1 Issue – Discussion

On May 16, 2011, researchers Billy Rios and Terry McCorkle reported a possible security related vulnerability in the GENESIS32™ product. This vulnerability is a design issue in a GENESIS32 ActiveX control that can set an arbitrary domain to the trusted zone.

ICONICS validated the researcher's claims for the 9.21 version of GENESIS32 and worked with the researchers on patch validation. ICONICS has released a downloadable patch, as well as steps listed below, to further mitigate this vulnerability. The patch for 9.2 can be downloaded at the ICONICS Support Web site, http://www.iconics.com/certs. This issue is addressed in GENESIS32 version 9.22 as well.

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

6.2 Products Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32™ and BizViz V9.21 Workbench32 and WebHMI	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Remote Code Execution	High

6.3 Impact

A successful exploit of the SetTrustedZone Policy vulnerability could result in an arbitrary domain getting into the trusted zone, consequently giving the ability to execute remote code. 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

The discovered vulnerability exists in the Workbench32 and WebHMI components (IcoSetServer.cab and default.htm) of GENESIS32 and BizViz. Exploitation of the Workbench32/WebHMI SetTrustedZone Policy vulnerability requires creation of a Web site that can load and use the IcoSetServer ActiveX control in a way that inserts an arbitrary domain into the Trusted Zone.

EXPLOITABILITY:
These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT:
There is no known exploit code specifically targeting these vulnerabilities.

DIFFICULTY:
The SetTrustedZone Policy vulnerability exploit would require development of a malicious application that has access to a GENESIS32 or BizViz Server machine hosting Workbench32 or WebHMI. The malicious application would need to pass a specially crafted string to a certain method of the IcoSetServer dll.

6.5 Mitigation

ICONICS is releasing a patch for the GENESIS32™ and BizViz™ V9.21 Workbench32/WebHMI that addresses the SetTrustedZone Policy vulnerability.

ICONICS recommends that users of GENESIS32™ and BizViz™ 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 patches.

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 GENESIS32 Write AV (ICS-CERT Advisory 11-273-01)

7.1 Issue – Discussion

In May and June, 2011, researchers Billy Rios and Terry McCorkle reported a number of write access violations and potential memory corruption vulnerabilities in some of the components that are part of GENESIS32 V9.21. The components include ScriptWorX32 v9.21, GraphWorx32 v9.21, the TrendWorX32 v9.21 container, and the AlarmWorX32 v9.21 container. Exploiting these vulnerabilities can cause a crash and could potentially allow arbitrary code execution.

ICONICS validated the researcher's claims that ScriptWorX32, GraphWorX32 and AlarmWorX32 are vulnerable to write access violations that can cause memory corruption, and validated the researcher's claim that that TrendWorX32 v9.21 is vulnerable to a memory corruption issue. ICONICS has released a downloadable patch, as well as steps listed below, to mitigate these vulnerabilities. This patch for version 9.2 can be downloaded at the ICONICS Support Web site, http://www.iconics.com/certs, and additional patches as described herein will be available shortly at the same web site.

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

7.2 Products Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32™ V8.05, V9.0, V9.1 and V9.2 – ScriptWorX32, AlarmWorX32 Container, and TrendWorX32 Container	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Denial of Service Possible code execution	High
GENESIS32™ V9.2 – GraphWorX32	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Denial of Service Possible code execution	High

7.3 Impact

A successful exploit of the ScriptWorX32, GraphWorX32, or AlarmWorX32 write access violation can cause a crash in the particular application. It could potentially allow arbitrary code execution.

A successful exploit of the TrendWorX32 container memory corruption issue can cause denial of service of TrendWorX32. It could potentially allow 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 this vulnerability based on their environment, architecture, and product implementation.

7.4 Vulnerability

The discovered vulnerabilities exists in the ScriptWorX32, GraphWorX32, AlarmWorX32 container, and TrendWorX32 container components of GENESIS32.

Exploitation of the ScriptWorX32 vulnerability requires creation of a specially crafted ScriptWorX3.swx file. Exploitation of the GraphWorX32 vulnerability requires creation of a specially crafted GraphWorX32 gdf file. Exploitation of the AlarmWorX32 container vulnerability requires creation of a specially crafted AlarmWorX32 a32 file. Exploitation of the TrendWorX32 container vulnerability requires creation of a specially crafted TrendWorX32 t32 file.

EXPLOITABILITY:
These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT
There is no known exploit code specifically targeting these vulnerabilities.

DIFFICULTY
An attacker with a moderate skill level can create the Denial of Service whereas it would require at least an advanced skill level to perform a code-execution exploit of any of the fore-mentioned vulnerabilities.

The ScriptWorX32 Code-Execution vulnerability exploit would require development of a malicious application that has access to a GENESIS32 system, an understanding of the ScriptWorX32.swx file format, and the skills to turn a write access violation/program crash into arbitrary code execution.

The GraphWorX32 Code-Execution vulnerability exploit would require development of a malicious application that has access to a GENESIS32 system, an understanding of the GraphWorX32 gdf file format, and the skills to turn a write access violation/program crash into arbitrary code execution.

The AlarmWorX32 Code-Execution vulnerability exploit would require development of a malicious application that has access to a GENESIS32 system, an understanding of the AlarmWorX32 a32 file format, and the skills to turn a write access violation/program crash into arbitrary code execution.

The TrendWorX32 Code-Execution vulnerability exploit would require development of a malicious application that has access to a GENESIS32 system, an understanding of the TrendWorX32 t32 file format, and the skills to turn the memory corruption into arbitrary code execution.

7.5 Mitigation

ICONICS is releasing patches for the GENESIS32 ScriptWorX32, the TrendWorX32 container, and AlarmWorX32 container for versions 8.05, 9.01, 9.13 9.21 that protects against the write access violation and potential crash. ICONICS is releasing a patch for the GENESIS32 GraphWorX32 component for version 9.2 that protects against the write access violation and potential crash.

ICONICS recommends that users of GENESIS32™ 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.

8 Authentication Bypass (ICS-CERT Advisory 12-212-01)

8.1 Issue – Discussion

On July 20, 2012, an anonymous researcher reported a possible security related vulnerability in the GENESIS32™ product, in the Security Configurator. The Security Configurator's User interface normally requires an administrative login. However, this can be bypassed with the assistance of ICONICS Technical Support if a legitimate user is locked out. This bypass is done by providing a challenge number to Tech Support, who can provide the correct response (after correctly verifying the customer's identity). However, a savvy attacker may be able to come up with a valid response on their own due to a limitation in the encryption algorithm being used.

ICONICS validated the researcher's claims for the 9.22 version of GENESIS32 and is working with US-CERT on patch validation. ICONICS has released a downloadable patch, as well as steps listed below, to further mitigate this vulnerability. This patch for 9.22 can be downloaded at the ICONICS Support Web site, http://www.iconics.com/certs, and additional patches as described herein will be available shortly at the same Web site.

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

8.2 Products Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32™ and BizViz V8.05, V9.0, V9.1 and V9.2 – Security Configurator	Windows XP, Windows 7, Windows Server 2003, Windows Server 2008	Unauthorized elevation of a user's security privileges	High

8.3 Impact

A successful exploit of the Security Configurator vulnerability could give a non-administrator user administrative privileges. 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

The discovered vulnerability exists in the security related components of GENESIS32 and BizViz. Exploitation of the Security Configurator vulnerability requires knowledge of the encryption algorithm being used for the backdoor challenge-code response, and knowledge on how to exploit the encryption algorithm.

EXPLOITABILITY:
This vulnerability is not remotely exploitable.

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

DIFFICULTY
An attacker with moderate skill level and knowledge of the encryption algorithm used to secure the challenge response may be able to obtain administrator privileges in the system.

8.5 Mitigation

ICONICS is releasing a patch for the GENESIS32™ and BizViz™ security files for versions 8.05, 9.01, 9.13, and 9.22 that disable the backdoor security login. In the future, this feature will be re-implemented with a more secure encryption algorithm.

ICONICS recommends that users of GENESIS32™ and BizViz™ 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.

9 Insecure ActiveX Cntrl (ICS-CERT Advisory 14-051-01)

9.1 Issue – Discussion

On January 9, 2014, ICS-CERT reported a possible security related vulnerability in the GENESIS32™ product, in the IcoLaunch.dll module. The IcoLaunch.dll was intended to launch GENESIS32 applications. However, an attacker could use the IcoLaunch.dll to launch any application, including a malicious application, via a command line or through an HTML page. It is noted that even though IcoLaunch.dll is an ActiveX control, it is not delivered over the Web and is only installed as part of a GENESIS32 V8 or earlier installation.

ICONICS validated the researcher's claims for the 8.05 version of GENESIS32 and is working with US-CERT on patch validation. ICONICS has released a downloadable patch, as well as steps listed below, to further mitigate this vulnerability. This patch for all version 8 (8.0, 8.02, 8.04, 8.05) products can be downloaded at the ICONICS Support Web site, http://www.iconics.com/certs, and additional patches if needed can be made available upon request.

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

9.2 Products Effected

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

Product and Component	Supported Operating System	Security Impact	Severity Rating
GENESIS32™ V8.05, IcoLaunch.dll	Windows XP, Windows Server 2003	Unauthorized Code Execution	High

9.3 Impact

A successful exploit of the IcoLaunch.dll vulnerability could potentially allow 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 this vulnerability based on their environment, architecture, and product implementation.

9.4 Vulnerability

The discovered vulnerability exists in the IcoLaunch component of GENESIS32. Exploitation of the IcoLaunch vulnerability requires some basic knowledge of HTML, and requires social engineering to get a user to load a malicious Web page.

EXPLOITABILITY:
This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT
There is no known exploit code specifically targeting this GENESIS32 vulnerability.

DIFFICULTY
Requires an attacker with moderate skill level and knowledge of HTML.

9.5 Mitigation

ICONICS is releasing a patch for GENESIS32™ version 8 (applicable to any v8 system)

ICONICS recommends that users of GENESIS32™ V8 systems 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 developer offering real-time visualization, HMI/SCADA, energy, fault detection, manufacturing intelligence, MES and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70% of the Fortune 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality and be more sustainable.

ICONICS products are used in building automation, oil & gas, renewable energy, utilities, water/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 300,000 applications installed in multiple industries worldwide.

World Headquarters
100 Foxborough Blvd.
Foxborough, MA, USA, 02035
Tel: 508 543 8600
Email: us@iconics.com
Web: www.iconics.com

Czech Republic
Tel: 420 377 183 420
Email: czech@iconics.com

Italy
Tel: 39 010 46 0626
Email: italy@iconics.com

Germany
Tel: 49 2241 16 508 0
Email: germany@iconics.com

Netherlands
Tel: 31 252 228 588
Email: holland@iconics.com

France
Tel: 33 4 50 19 11 80
Email: france@iconics.com

UK
Tel: 44 1384 246 700
Email: uk@iconics.com

Australia
Tel: 61 2 9727 3411
Email: australia@iconics.com

China
Tel: 86 10 8494 2570
Email: china@iconics.com

India
Tel: 0091 22 67291029
Email: india@iconics.com

Microsoft Partner
Gold Application Development

2013 Microsoft Partner of the Year Award Finalist
Application Development

VISUALIZE ANALYZE MOBILIZE

64 Windows 8 Compatible Compatible with Windows 7 Windows Server 2012 Certified BTL CERTIFIED OPC vmware READY

Further information:
www.iconics.com