



**MITSUBISHI ELECTRIC  
ICONICS DIGITAL SOLUTIONS, INC.**

WHITEPAPER ON GENESIS32 AND BizViz (V9) SECURITY  
VULNERABILITIES – JANUARY 2026

# CONTENTS

<b>1</b>	<b>OVERVIEW .....</b>	<b>3</b>
<b>2</b>	<b>GENBROKER (ICS-CERT ALERT 11-080-02).....</b>	<b>5</b>
<b>3</b>	<b>SAFENET LICENSING DRIVER (ICS-CERT ADVISORY 11-108-01) .....</b>	<b>7</b>
<b>4</b>	<b>WEBHMI (ICS-CERT ADVISORY 11-131-01).....</b>	<b>8</b>
<b>5</b>	<b>SECURITY LOGIN (ICS-CERT ADVISORY 11-182-02) .....</b>	<b>9</b>
<b>6</b>	<b>SETTRUSTEDZONE POLICY (ICS-CERT ADVISORY 11-182-01) .....</b>	<b>10</b>
<b>7</b>	<b>GENESIS32 WRITE AV (ICS-CERT ADVISORY 11-273-01) .....</b>	<b>11</b>
<b>8</b>	<b>AUTHENTICATION BYPASS (ICS-CERT ADVISORY 12-212-01) .....</b>	<b>13</b>
<b>9</b>	<b>INSECURE ACTIVEX CONTROL (ICS-CERT ADVISORY 14-051-01) .....</b>	<b>15</b>
<b>10</b>	<b>GENBROKER OOB (ICS-CERT ADVISORY 20-170-03) .....</b>	<b>16</b>
<b>11</b>	<b>SQL QUERY ENGINE BUFFER OVER-READ (ICS-CERT ADVISORY 22-020-01) .....</b>	<b>17</b>
<b>12</b>	<b>GENBROKER DESERIALIZATION OF UNTRUSTED DATA (ICS-CERT ADVISORY 22-202-04) 18</b>	
<b>13</b>	<b>GENBROKER OUT-OF-BOUNDS READ (ICS-CERT ADVISORY 22-202-04) .....</b>	<b>19</b>
<b>14</b>	<b>ALARMWORX MMX DLL HIJACKING (ICS-CERT ADVISORIES 24-338-04, 24-184-03)20</b>	
<b>15</b>	<b>ICONICS LICENSING DLL HIJACKING (ICS-CERT ADVISORY 24-184-03).....</b>	<b>21</b>
<b>16</b>	<b>GENBROKER32 INSTALLATION PERMISSIONS ISSUE (ICS-CERT ADVISORY 24-296-01) 22</b>	
<b>17</b>	<b>INFORMATION TAMPERING VULNERABILITY IN GENESIS32 (ICS-CERT ADVISORY 25-140-04) .....</b>	<b>24</b>
<b>18</b>	<b>DEPRECATED COMPONENTS IN GENESIS32 AND BIZVIZ .....</b>	<b>26</b>

# 1 Overview

---

Mitsubishi Electric Iconics Digital Solutions takes extraordinary efforts in testing and validating its software before it is released. Unfortunately, there are instances where security vulnerabilities are discovered, either internally, or by external researchers. Mitsubishi Electric Iconics Digital Solutions takes such issues very seriously. All such vulnerabilities are documented, assigned to engineering teams for investigation and validation, and addressed as quickly as reasonably possible and in accordance with the Software Lifecycle Policy. Once fully tested, software updates for the current release and, in some cases, past releases, are posted to the company's Community Portal. Information on the updates is provided on the following website:

<https://www.iconics.com/cert>

Mitsubishi Electric Iconics Digital Solutions coordinates with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on these issues. The following table lists all vulnerabilities that are described in this document. This document is updated as new issues are discovered, validated, addressed and have been disclosed.

Section	Vulnerability Issue
2	GenBroker in ICONICS' GENESIS32™ products (ICS-Alert-11-080-02)
3	SafeNet Licensing Driver in GENESIS32 and BizViz (ICSA-11-108-01)
4	WebHMI buffer overflow in GENESIS32 and BizViz (ICSA-11-131-01)
5	Security Login Buffer Overflow (ICSA-11-182-02)
6	SetTrustedZone Policy in GENESIS32 and BizViz (ICSA-11-182-01)
7	GENESIS32 Write Access Violation (ICSA-11-273-01)
8	Authentication Bypass in GENESIS32 and BizViz (ICSA-12-212-01)
9	Insecure ActiveX Control in GENESIS32 (ICSA-14-051-01)
10	GenBroker Out-of-bounds (ICSA-20-170-03)
11	SQL Query Engine Buffer Over-read (ICSA-22-020-01)
12	GenBroker Deserialization of Untrusted Data (ICSA-22-202-04)
13	GenBroker Out-of-Bounds Read (ICSA-22-202-04)
14	AlarmWorX MMX DLL Hijacking (ICSA-24-338-04, ICSA-24-184-03)
15	ICONICS Licensing DLL Hijacking (ICSA-24-184-03)
16	GenBroker32 Installation Permissions Issue (ICSA-24-296-01)
17	Information Tampering Vulnerability in GENESIS32 (ICSA 25-140-04)
18	Deprecated Components in GENESIS32 and BizViz

Mitsubishi Electric Iconics Digital Solutions GENESIS32™ 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/wastewater, 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.

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the latest version of Mitsubishi Electric Iconics Digital Solutions GENESIS product and keep it up to date with the latest releases. The latest version, Version 11, was released in February 2025. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Mitsubishi Electric Iconics Digital Solutions 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.

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

---

**2.1 Date:** May 2011

### 2.2 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.

Mitsubishi Electric Iconics Digital Solutions 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, <https://www.iconics.com/cert>.

### 2.3 Products Affected

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

### 2.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

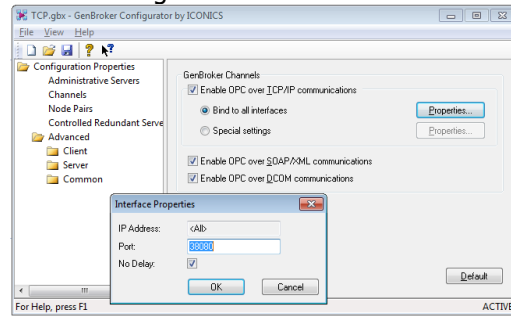
### 2.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions 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.



Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its Web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 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 Mitsubishi Electric Iconics Digital Solutions 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

### 3.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

### 3.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions has released an updated version of the SafeNet Sentinel Protection Server (v7.6.4) that addresses the directory traversal vulnerability. Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its Web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

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

---

**4.1 Date:** May 2011

### 4.2 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. Mitsubishi Electric Iconics Digital Solutions validated the researcher’s claims for the 9.21 version of WebHMI which is part of the GENESIS32 and BizViz V9.21 product families. Mitsubishi Electric Iconics Digital Solutions 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 Mitsubishi Electric Iconics Digital Solutions Support Web site, <https://www.iconics.com/cert>, and additional patches as described herein will be available shortly at the same Web site.

### 4.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products that may be affected.

<b>Product and Component</b>	<b>Supported Operating System</b>	<b>Security Impact</b>	<b>Severity Rating</b>
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

### 4.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

### 4.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions released 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. Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its Web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 5 Security Login (ICS-CERT Advisory 11-182-02)

---

**5.1 Date:** May 2011

### 5.2 Issue – Discussion

On May 10, 2011, researchers Billy Rios and Terry McCorkle reported a potential crash in the Security Login controls used by GENESIS32 due to a buffer overrun. Mitsubishi Electric Iconics Digital Solutions validated the researcher’s claims for the 9.21 version of GENESIS32. Mitsubishi Electric Iconics Digital Solutions 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 Mitsubishi Electric Iconics Digital Solutions Support Web site, <https://www.iconics.com/cert>. This issue is addressed in GENESIS32 version 9.22 as well.

### 5.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products that may be affected.

<b>Product and Component</b>	<b>Supported Operating System</b>	<b>Security Impact</b>	<b>Severity Rating</b>
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

### 5.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 5.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions released 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. Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its Web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions 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.

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

---

**6.1 Date:** May 2011

### 6.2 Issue – Discussion

On May 16, 2011, researchers Billy Rios and Terry McCorkle reported a security 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. Mitsubishi Electric Iconics Digital Solutions validated the researcher’s claims for the 9.21 version of GENESIS32. Mitsubishi Electric Iconics Digital Solutions 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 Mitsubishi Electric Iconics Digital Solutions Support Web site, <https://www.iconics.com/cert>. This issue is addressed in GENESIS32 version 9.22 as well.

### 6.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions 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

### 6.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 6.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions released a patch for the GENESIS32™ and BizViz™ V9.21 Workbench32/WebHMI that addresses the SetTrustedZone Policy vulnerability. Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

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

---

**7.1 Date:** September 2011

### 7.2 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.

Mitsubishi Electric Iconics Digital Solutions 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. Mitsubishi Electric Iconics Digital Solutions 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 Mitsubishi Electric Iconics Digital Solutions Support Web site, <https://www.iconics.com/cert>.

### 7.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products that may be affected.

<b>Product and Component</b>	<b>Supported Operating System</b>	<b>Security Impact</b>	<b>Severity Rating</b>
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

### 7.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 7.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions released 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. Mitsubishi Electric Iconics Digital Solutions is releasing a patch for the GENESIS32 GraphWorX32 component for version 9.2 that protects against the write access violation and potential crash.

Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

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

---

**8.1 Date:** July 2012

### 8.2 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 Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions validated the researcher's claims for the 9.22 version of GENESIS32 and is working with US-CERT on patch validation. Mitsubishi Electric Iconics Digital Solutions 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 Mitsubishi Electric Iconics Digital Solutions Support Web site, <https://www.iconics.com/cert>.

### 8.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions 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

### 8.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 8.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions released 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.

Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

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

---

**9.1 Date:** February 2014

### 9.2 Issue – Discussion

On January 9, 2014, ICS-CERT reported a security 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.

Mitsubishi Electric Iconics Digital Solutions validated the researcher's claims for the 8.05 version of GENESIS32 and is working with US-CERT on patch validation. Mitsubishi Electric Iconics Digital Solutions 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 Mitsubishi Electric Iconics Digital Solutions Support Web site, <https://www.iconics.com/cert>.

### 9.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions 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

### 9.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 9.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions released a patch for GENESIS32™ version 8 (applicable to any v8 system). Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 10 GenBroker OOB (ICS-CERT Advisory 20-170-03)

---

**10.1 Date:** June 2020

### 10.2 Issue – Discussion

On January 21, 2020, researchers Tobias Scharnowski, Niklas Breinfeld, and Ali Abbasi reported a security vulnerability in the GENESIS64 GenBroker64 module. Mitsubishi Electric Iconics Digital Solutions validated the researcher’s claims that GenBroker64 is susceptible to an Out of Bounds condition, which if exploited, can result in remote code execution. This Out of Bounds condition also exists in GenBroker, the GENESIS32 version of GenBroker64.

Mitsubishi Electric Iconics Digital Solutions 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 Mitsubishi Electric Iconics Digital Solutions web site, <https://www.iconics.com/cert>.

### 10.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products that may be affected.

Product and Component	Version	Security Impact	Severity Rating
GenBroker32 contained in the products: <ul style="list-style-type: none"><li>• GENESIS32</li><li>• BizViz</li></ul>	All versions up to and including V9.5	Out of Bounds Possible remote code execution	A CVSS v3 base score of 8.1 was calculated

### 10.4 Impact

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

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

### 10.5 Mitigation

Mitsubishi Electric Iconics Digital Solutions released a patch for version V9.5.

Mitsubishi Electric Iconics Digital Solutions 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates, as well as the patch described above, at its web site at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 11 SQL Query Engine Buffer Over-read (ICS-CERT Advisory 22-020-01)

---

**11.1 Date:** January 2026

### 11.2 Issue – Discussion

This security vulnerability makes it possible to execute a series of SQL commands in a GENESIS32 system that can cause a crash of the SQL Query Engine and ultimately can result in a disabling of SQL Server. The issue is a result of a coding error in the SQL Query Engine memory allocation code.

### 11.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GENESIS32	All versions up to and including 9.7	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

### 11.4 Impact

A successful exploit of this vulnerability can potentially result in a crash of the SQL Query Engine and ultimately can result in a disabling of SQL Server. The specific impact to an organization depends on many factors unique to that organization. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 11.5 Mitigation

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on version 9 should be aware of this vulnerability and should take any necessary precautions to keep the system safe from potential attackers such as:

- Configure the PCs with the affected product installed so that only trusted users are given the credentials to the SQL Server where the SQL Query Engine is installed.
- Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.
- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 12 GenBroker Deserialization of Untrusted Data (ICS-CERT Advisory 22-202-04)

---

**12.1 Date:** January 2026

### 12.2 Issue – Discussion

Researcher Axel 'Overcl0k' Souchet working with Trend Micro Zero Day Initiative, reported a deserialization issue in GENESIS64 GenBroker64 where if exploited, can result in remote code execution. Mitsubishi Electric Iconics Digital Solutions determined this issue is also present in GENESIS32 GenBroker.

### 12.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GenBroker contained in GENESIS32 V9	All versions up to and including 9.7	Possible remote code execution	9.8 (AV:N/AC:L/P R:N/UI:N/S:U/ C:H/I:H/A:H)	502 - Deserialization of Untrusted Data	CVE-2022-33318

### 12.4 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. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 12.5 Mitigation

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on affected versions should be aware of this information tampering vulnerability and take any necessary precautions to keep the system safe from potential attackers such as:

- Block unauthorized access by using a firewall or virtual private network (VPN).
- Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.
- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 13 GenBroker Out-of-Bounds Read (ICS-CERT Advisory 22-202-04)

---

**13.1 Date:** January 2026

### 13.2 Issue – Discussion

Researcher Axel 'Overcl0k' Souchet, working with Trend Micro Zero Day Initiative, reported an out-of-bounds read issue in GENESIS64 GenBroker64 where if exploited, can result in information disclosure or potentially a crash of GenBroker64 and a denial-of-service issue. Mitsubishi Electric Iconics Digital Solutions determined this issue is also present in GENESIS32 GenBroker.

### 13.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS V3.1 Base Score	CWE	CVE
GenBroker contained in GENESIS32 V9	All versions up to and including 9.7	Information Disclosure, Possible denial of service	8.2 (AV:N/AC:L/P R:N/UI:N/S:U /C:L/I:N/A:H)	125 - Out-of-bounds Read	CVE-2022-33319

### 13.4 Impact

A successful exploit of this vulnerability can potentially result in information disclosure or a crash of GenBroker and consequently, a denial of service. The specific impact to an organization depends on many factors unique to that organization. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 13.5 Mitigation

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on affected versions should be aware of this information tampering vulnerability and take any necessary precautions to keep the system safe from potential attackers such as:

- Block unauthorized access by using a firewall or virtual private network (VPN).
- Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.
- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 14 AlarmWorX MMX DLL Hijacking (ICS-CERT Advisories 24-338-04, 24-184-03)

---

**14.1 Date:** January 2026

### 14.2 Issue – Discussion

Researchers Asher Davila and Malav Vyas at Palo Alto Networks reported multiple DLL hijacking vulnerabilities in GENESIS64 AlarmWorX64 MMX. An attacker exploiting these vulnerabilities would be able to trick the system into loading a malicious DLL file, allowing the attacker to potentially execute arbitrary code. Mitsubishi Electric Iconics Digital Solutions investigated this issue and determined it is present in the GENESIS32 AlarmWorX MMX product, specifically in the MMX Fax, Pager, and MMX Phone Agents.

### 14.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products and versions that may be affected.

Product	Version	Security Impact	CVSS 3.1	CWE	CVE
AlarmWorX MMX Pager, Phone, and Fax Agents	All versions	Potential Arbitrary Code Execution	7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	427 – Uncontrolled Search Path Element	CVE-2024-1182 CVE-2024-8299 CVE-2024-9852

### 14.4 Impact

The impact of a successful exploit of this vulnerability is that an attacker can cause arbitrary malicious code execution. The specific impact to an organization depends on many factors unique to that organization. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 14.5 Mitigation

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on affected versions should be aware of this information tampering vulnerability and take any necessary precautions to keep the system safe from potential attackers such as:

- Block unauthorized access by using a firewall or virtual private network (VPN).
- Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.
- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 15 ICONICS Licensing DLL Hijacking (ICS-CERT Advisory 24-184-03)

**15.1 Date:** January 2026

### 15.2 Issue – Discussion

There is a vulnerability in the ICONICS licensing software that can potentially allow a privilege escalation issue.

### 15.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS	CWE	CVE
GENESIS32, BizViz	All versions up to and including 9.7	Improper Authorization	6.7 CSSV:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	CVE-2024-1574

### 15.4 Impact

The impact of a successful exploit of this vulnerability would allow privilege escalation of any regular user to LOCALSYSTEM. The specific impact to an organization depends on many factors unique to that organization. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### 15.5 Mitigation

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on affected versions should be aware of this information tampering vulnerability and take any necessary precautions to keep the system safe from potential attackers such as:

- Block unauthorized access by using a firewall or virtual private network (VPN).
- Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.
- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

# 16 GenBroker32 Installation Permissions Issue (ICS-CERT Advisory 24-296-01)

**16.1 Date:** January 2026

## 16.2 Issue – Discussion

Researchers Asher Davila and Malav Vyas at Palo Alto Networks reported the existence of a permissions issue in the GenBroker32 installation. Mitsubishi Electric Iconics Digital Systems investigated this report and determined that all versions of the GenBroker32 installation included in the Version 9 releases, up to and including v9.7, incorrectly set the permissions on the C:\ProgramData\ICONICS folder to “Everyone”.

Mitsubishi Electric Iconics Digital Solutions has addressed this issue in the 9.70.300.32 version of the GenBroker32 installation, which is available on the company’s support web site.

## 16.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS	CWE	CVE
GenBroker32	All versions earlier than 9.70.300.32	Disclosure of Information, data tampering, and Denial of Service (DoS)	7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	276 – Incorrect Default Permissions	CVE-2024-7587

## 16.4 Impact

A successful exploit of this vulnerability can lead to the disclosure of confidential information contained in these products, data tampering, or a denial of service (DoS) condition. The specific impact to an organization depends on many factors unique to that organization. Mitsubishi Electric Iconics Digital Solutions recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

## 16.5 Mitigation

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on version 9 should be aware of this folder permissions vulnerability and take the following mitigation steps:

- For new systems, do not use the GenBroker that comes with GENESIS32 or BizViz. Instead, download the latest GenBroker32 (version 9.70.300.32 or higher) from Mitsubishi Electric Iconics Digital Solutions and install this version as needed.
- For systems that already have v9 installed, verify the permissions on the C:\ProgramData\ICONICS folder do not include “Everyone”. If this folder is set to provide access to “Everyone”, remove this access by performing the following steps:
  1. Right click C:\ProgramData\ICONICS folder and open the Properties display
  2. Open the Security tab

3. Click Advanced
  4. Click Change Permissions
  5. Select "Everyone" and check the "Replace all object permissions entries with inheritable permission entries from this project" checkbox
  6. Click Remove
- Don't open files from untrusted sources.
  - 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

# 17 Information Tampering Vulnerability in GENESIS32 (ICS-CERT Advisory 25-140-04)

**17.1 Date:** January 2026

## 17.2 Issue – Discussion

Researchers Asher Davila and Malav Vyas at Palo Alto Networks reported the existence of an elevation of privilege vulnerability that can result in information tampering in the AlarmWorX64 MMX Pager Agent in GENESIS64. An attacker could make an unauthorized write to arbitrary files by creating a symbolic link to a file used as a write destination by the Pager Agent service of GENESIS64. This could allow the attacker to destroy the file on a PC with GENESIS64 installed (CVE-2025-0921), resulting in a denial-of-service (DoS) condition on the PC.

Mitsubishi Electric Iconics Digital Solutions verified this vulnerability exists in GENESIS64 and determined that it also exists in the GENESIS32 AlarmWorX MMX Pager Agent, as well as in other services included in GENESIS32 and BizViz.

## 17.3 Products Affected

Product	Version	Security Impact	CWE	CVE
GENESIS32 and BizViz	All Versions	Unauthorized write to arbitrary files	250 – Execution with Unnecessary Privileges	CVE-2025-0921

**CVSS V3.1 Base Score:** 6.5 (AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N)

**CVSS V4.0 Base Score:** 8.3 (AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H)

## 17.4 Impact

An attacker could make an unauthorized write to arbitrary files, by creating a symbolic link to a file used as a write destination by a GENESIS32 or BizViz service. This could allow the attacker to destroy the file on a PC with GENESIS32 or BizViz installed (CVE-2025-0921), resulting in a denial-of-service (DoS) condition on the PC if the destroyed file is necessary for the operation of the PC.

## 17.5 Mitigations

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 applications, depending on which applications are being used, with different V11 applications. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on version 9 should be aware of this vulnerability and take any necessary precautions including:

- Configure the PCs with the affected product installed so that only an administrator can log in.
- PCs with the affected product installed should be configured to block remote logins from untrusted networks and hosts, and from non-administrator users.
- Block unauthorized access by using a firewall or virtual private network (VPN), etc., and allow remote login only to administrators when connecting the PCs with the affected product installed to the Internet.
- Restrict physical access to the PC with the affected product installed and the network to which the PC is connected to prevent unauthorized physical access.

- Do not click on web links in emails from untrusted sources. Also, do not open attachments in untrusted emails.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.

## 18 Deprecated Components in GENESIS32 and BizViz

---

**18.1 Date:** January 2026

### 18.2 Issue – Discussion

GENESIS32 and BizViz include (or in some cases are based on) a number of Microsoft components that are in a deprecated state. The deprecated Microsoft components include:

- Microsoft Visual Studio 2005 Redistributable
- Microsoft Visual Studio 2008 Redistributable
- PowerShell 2.0
- Microsoft .NET Framework 2.0
- Microsoft Data Access Components (MDAC)
- Microsoft SQL Server 2012 SP2

### 18.3 Products Affected

The following table identifies Mitsubishi Electric Iconics Digital Solutions products and versions that may be affected.

Product / Component	Version	Security Impact	CVSS	CWE	CVE
GENESIS32, BizViz	All versions up to and including 9.7	Unknown	NA	NA	NA

### 18.4 Impact

The above listed components that have been deprecated by Microsoft are no longer supported or maintained. This means that they may have vulnerabilities that are not being patched, making the software susceptible to attacks. Additionally, these components can potentially have compatibility issues with newer systems and could have reduced overall performance.

### 18.5 Mitigation

Version 9 products are in the Retired Stage of the [Product Lifecycle Policy](#). As described in the policy, these versions are no longer monitored for security vulnerabilities, nor are they being fixed or patched. Please see the Product Lifecycle Policy for full details.

For the highest level of security, it is recommended that users use the Current Development version of Mitsubishi Electric Iconics Digital Solutions products as defined in [Product Lifecycle Policy](#) (GENESIS V11 at the time of this writing) and keep it up to date with the latest releases. Note, upgrading to V11 may require replacing some of the V9 components with newer V11 components. Please consult Mitsubishi Electric Iconics Digital Solutions on the options for upgrades.

Users who remain on version 9 should be aware of these deprecated components and take any necessary precautions including:

- 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.

Mitsubishi Electric Iconics Digital Solutions provides information and useful links related to its security updates on its website at <https://www.iconics.com/cert>. Mitsubishi Electric Iconics Digital Solutions is committed to providing high-quality secure products to its customers.