Security Bulletin

Overview

ARC Informatique is aware of 5 security vulnerabilities affecting its products.
One security vulnerability has been privately reported to the ICS-CERT by a security expert. The 4 others have been publicly disclosed along with proof-of-concept (PoC) exploit code.
We have been working in coordination with the ICS-CERT to confirm these vulnerabilities and provide you with risk mitigation.
This bulletin describes the immediate security measures to prevent the malicious exploitation of these vulnerabilities. We strongly recommend that users of the affected products apply these measures.

The ICS-CERT has validated these security measures and confirmed that they resolve the identified vulnerabilities.

Affected products and components

Component	Product	Description
SVUIGrd.ocx	PcVue - From version 6.00 onward Starting with PcVue 9.0 SP2 and PcVue 10.0 updates kill-bits are set by the installation package and the Component Registration Utility. The vulnerable component is no longer installed with PcVue 10.0 SP1, 11 and later versions.	An ActiveX supplied with PcVue. File location: $InstallationDirectory$\Bin\SVUIGrd.ocx. CLSID: {2BBD45A5-28AE-11D1-ACAC-0800170967D9}
aipgctl.ocx	PcVue - From version 7.00 onward FrontVue - All versions PlantVue - All versions Starting with PcVue 9.0 SP2, PcVue 10.0 updates and corresponding FrontVue versions, kill-bits are set by the installation package and the Component Registration Utility.	An ActiveX supplied with PcVue, FrontVue and PlantVue. File location: Windows system folders. CLSID: {083B40D3-CCBA-11D2-AFE0-00C04F7993D6}

Table 1 - Affected products and components

Impact

By convincing a user to view a specially crafted HTML document or HTML mail message, an attacker could remotely execute arbitrary code with the privileges of the user logged-in the targeted system. Note that the affected software does not need to be running for this vulnerability to be exploited.

Successful exploitation of these vulnerabilities may have the following impact:

- Denial-Of-Service
- Potential to write memory
- Possible file corruption
- Possible remote code execution

The exact impact on a particular system depends on many factors. According to the vulnerabilities described hereafter, we recommend that each user of the affected products evaluates the risk for their system.

Vulnerability details

A total of 5 vulnerabilities have been reported, affecting the *SVUIGrd.ocx* and *aipgctl.ocx* components.

Id	Type	Exploitability	Existence of exploit	Component
#1	Integer Overflow	Remotely exploitable	Yes	SVUIGrd.ocx
#2	Control of a function pointer	Remotely exploitable	Yes - Public	SVUIGrd.ocx
#3	Arbitrary memory write	Remotely exploitable	Yes - Public	SVUIGrd.ocx
#4	Directory traversal	Remotely exploitable	Yes - Public	SVUIGrd.ocx
#5	Array overflow	Remotely exploitable	Yes - Public	aipgctl.ocx

Table 2 – Vulnerability details

The vulnerabilities might be exploited when executing some of the ActiveX controls' methods with unexpected or specially crafted parameter values.
They take advantage of the fact that Internet Explorer 6 is still widely available on computers running Windows XP.

Immediate risk mitigation

In addition to avoiding direct exposure of your system and users to the outside world, we recommend you to immediately apply the following measures.

Upgrade Microsoft Internet Explorer

Who should apply this recommendation: **All users**

An important factor of the risk of remote exploitation relies in the availability and use of Microsoft Internet Explorer 6.0 on the affected system, or an inadequate configuration of the Microsoft web browser.

The first measure to take is to upgrade all computers to a more recent version of Internet Explorer, and apply the required settings to prevent ActiveX and potentially harmful scripts to be loaded and executed in the Microsoft web browser. Starting with IE 7, the necessary options are available.

For more information about securing Internet Explorer web browsers with regards to ActiveX execution, please refer to the following US-CERT document: Securing your Web browser.

Remove the affected component - SVUIGrd.ocx

Who should apply this recommendation: **All users not using the affected component**

The affected component is an obsolete table-like control, also called "Grid". This component was not used by the PcVue software itself: It is delivered and installed with PcVue as an optional control that could be embedded in HMI applications built and run using PcVue.

Since PcVue version 8.10 onward, we have made available a new control designed to replace *SVUIGrd.ocx*. Our compatibility policy led us to continue the shipping and installation of the obsolete one until now. Therefore, a large number of systems with PcVue installed may not use this component at all.

We recommend that all customers not using the *SVUIGrd.ocx* component in their HMI applications remove it from their system.

Removal procedure

Step 1: Locate the *SVUIGrd.ocx* file

- The default location is *$InstallationDirectory$\Bin\SVUIGrd.ocx where $InstallationDirectory$* is the installation folder.
  It is by default *C:\ARC Informatique\PcVue xx\Bin\* under recent operating systems such as Microsoft Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2.
  It is by default *C:\Program Files\ARC Informatique\PcVue xx\Bin\* under Windows XP and Windows Server 2003.
  xx refers to the PcVue version.

Step 2: Unregister the *SVUIGrd.ocx* ActiveX

- Launch the Windows command line tool (Cmd) – With administrator privileges
- Run the following commands to unregister the affected ActiveX:

```
cd $InstallationDirectory$\Bin\
Regsvr32.exe /u SVUIGrd.ocx
```

Step 3: Delete the *SVUIGrd.ocx* file

- Using the Windows file explorer, locate and delete the *SVUIGrd.ocx* file.

Warnings

Installing or re-installing one of the affected PcVue versions will install this component. The removal procedure should be executed in such instances.

If you follow this removal procedure, you will notice that the PcVue Component Registration Utility raises a warning due to the fact that the *SVUIGrd.ocx* component cannot be registered. It is a sign that the removal procedure was successful.

Prevent the execution of *SVUIGrd.ocx* and *aipgctl.ocx* in Microsoft Internet Explorer

Who should apply this recommendation: **All users**

In normal conditions, there is absolutely no reason to load and run the affected components in Internet Explorer.
Therefore, the technique known as "kill-bit" can be applied to completely prevent the affected components from being run in Internet Explorer.

Set up the kill-bit

Step 1: Download the *KillBits-SB2011-1.zip* file from the technical resources web site and extract the files it contents:

- If you use an x86 operating system, use *KillBits-SB2011-1-x86.reg*
- If you use an x64 operating system, use *KillBits-SB2011-1-x64.reg*

Step 2: Execute the adequate *.reg* file according to your system - Requires administrator privileges:

- Double-click on the *.reg* file to run it.

These *.reg* files add registry keys that will prevent loading and executing the *SVUIGrd.ocx* and *aipgctl.ocx* ActiveX controls, as well as other dependent components, in the context of various Microsoft tools such as Internet Explorer, Microsoft Office applications …

The files made available on the KB are compatible with the Windows Registry Editor Version 5.0 which is available with Microsoft operating systems since Windows 2000.

Warnings

These registry keys may be lost when installing or re-installing the operating system. Please make sure you also execute this procedure in such instances.

Available patches or updates

If using PcVue version 9.0 SP2, 10.0 updates and later versions:
The installation package and the PcVue Component Registration Utility apply the necessary kill-bits.

If using PcVue version 10.0 SP1, 11 and later versions:
The *SVUIGrd.ocx* component is no longer installed.

The same goes for the corresponding FrontVue versions.

References

The ICS-CERT alert: ICS-ALERT-11-271-01

The ICS-CERT advisory: ICSA-11-340-01

The public ARC Informatique security alert page: www.pcvuesolutions.com

The Knowledge Base article for more information: support.pcvuesolutions.com

Want to report a vulnerability or provide feedback – Please email us at secure@arcinfo.com

Document history

Revision	Action	Date
1.0	First publication	14/11/2011
1.1	Updated reference to the ICS-CERT advisory	03/01/2012
1.2	Update to section "Available patches or updates" after release of PcVue 10.0 SP1	17/11/2014