Overview

ARC Informatique is aware of a security vulnerability affecting ActiveBar, a third-party component installed as part of its products.
This bulletin describes the immediate security measures to prevent the malicious exploitation of this vulnerability. We strongly recommend that users of the affected products apply these measures.

Affected products and components

Component	Product	Description
ActBar.ocx	PcVue - From version 6.0 to 7.20 FrontVue – All versions prior to 3.1 PlantVue – All versions prior to 2.0 Starting with PcVue 9.0 SP3, PcVue 10.0 updates, PcVue 11 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: {E4F874A0-56ED-11D0-9C43-00A0C90F29FC}
ActBar2.ocx	PcVue - From version 8.00 to 9.0 SP2 and 10.0 FrontVue - From version 3.1 to 5.1 PlantVue - From version 2.0 onward Starting with PcVue 9.0 SP3, PcVue 10.0 updates, PcVue 11 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: {4932CEF4-2CAA-11D2-A165-0060081C43D9}

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.

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.

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.

Prevent the execution of *ActBar.ocx* and *ActBar2.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-SB2012-1.zip* file from the technical resources web site and extract the files it contents:

- If you use an x86 operating system, use *KillBits-SB2012-1-x86.reg*
- If you use an x64 operating system, use *KillBits-SB2012-1-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

Microsoft provided means of protection as part of an Update Rollup for ActiveX Kill Bits in August 2011. See Microsoft kb2562937 for more information.

Starting with PcVue 9.0 SP3, PcVue 10.0 updates, PcVue 11 and corresponding FrontVue versions, kill-bits are set by the installation package and the Component Registration Utility.

References

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

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

The Microsoft Security advisory: Microsoft Security Advisory 2562937

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

Document history

Revision	Action	Date
1.0	First publication	18/11/2014