SECURITY BULLETIN 2023-2

Microsoft Visual Basic for Applications vulnerability

SUMMARY :

This document contains information about a vulnerability in Microsoft Visual Basic for Applications runtime.

Reference	SB2023-2
Publication date	2024.05.02
Last update	2024.07.04
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2024.05.02	1.0	Initial version
2024.07.04	Rev A	(editorial) Updated document template (technical) Updated section “Available patches” (fix now available with 16.2.0)

1. Overview

ARC Informatique is aware of a security vulnerability affecting PcVue and FrontVue.

The vulnerable component is the Microsoft Visual Basic for Applications runtime provided with PcVue and FrontVue. The vulnerability consists in a Remote Code Execution and is linked to the CVE-2010-0815 and CVE-2012-1854 (Microsoft advisories MS10-031 and MS12-046).

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.

2. Affected products and components

Component	Product & Versions	Description
Microsoft Visual Basic for Applications	PcVue version 9.0 to 16.1 FrontVue version 4.2 to 16.1	Remote Code Execution

3. Impact

Based on the original description of the Microsoft Office CVEs, the impact in the context of PcVue and FrontVue is the following:
The vulnerability could allow remote code execution if a host application (PcVue or FrontVue) opens and passes a specially crafted file to the Visual Basic for Applications runtime, or if a specially crafted dll is located in the same directory as a legitimate mimic or VBA symbol. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full permissions. Users whose accounts are configured to have fewer permissions on the system could be less impacted than users who operate with administrative privileges.

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 evaluate the risk for their system.

4. Vulnerability details

4.1 VBE6.DLL Stack Memory Corruption

CVE Id	CVE-2010-0815		
Publication date	2010-05-12		
Description	VBE6.DLL in Microsoft Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Visual Basic for Applications (VBA), and VBA SDK 6.3 through 6.5 does not properly search for ActiveX controls that are embedded in documents, which allows remote attackers to execute arbitrary code via a crafted document, aka "VBE6.DLL Stack Memory Corruption Vulnerability."		
Impact	The vulnerability could allow remote code execution if a host application opens and passes a specially crafted file to the Visual Basic for Applications runtime. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.		
CVSS v2 Base Score	9.3		
CVSS v2 Vector	AV:N/AC:M/Au:N/C:C/I:C/A:C		
Attack Vector	Network	Adjacent	Local
Attack Complexity	Low	Medium	High
Authentication	None	Single	Multiple
Confidentiality	Complete	Partial	None
Integrity	Complete	Partial	None
Availability	Complete	Partial	None
CWE Ids	CWE-94: Improper Control of Generation of Code ('Code Injection')		

4.2 Memory leak

CVE Id	CVE-2012-1854		
Publication date	2010-07-10		
Description	Untrusted search path vulnerability in VBE6.dll in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Microsoft Visual Basic for Applications (VBA); and Summit Microsoft Visual Basic for Applications SDK allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .docx file, aka "Visual Basic for Applications Insecure Library Loading Vulnerability," as exploited in the wild in July 2012.		
Impact	The vulnerability could allow remote code execution if a user opens a legitimate Microsoft Office file (such as a .docx file) that is located in the same directory as a specially crafted dynamic link library (DLL) file. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.		
CVSS v2 Base Score	6.9		
CVSS v2 Vector	AV:L/AC:M/Au:N/C:C/I:C/A:C		
Attack Vector	Network	Adjacent	Local
Attack Complexity	Low	Medium	High
Authentication	None	Single	Multiple
Confidentiality	Complete	Partial	None
Integrity	Complete	Partial	None
Availability	Complete	Partial	None
CWE Ids	CWE-426: Untrusted Search Path		

5. Immediate risk mitigation

5.1 Harden the configuration

Who should apply this recommendation: All users

You should make sure project files are only accessible to authorized users. The system operators are highly recommended to take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls and isolate them from business networks.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.
- Minimize the level of privileges of the account used to run the product. Administrative privileges are only required at installation or for deployment purposes.

5.2 Apply the patch from Microsoft

Who should apply this recommendation: All users using the affected component
On every host computer where PcVue or FrontVue is installed, download and apply the KB2688865 patch from Microsoft.
https://www.microsoft.com/download/details.aspx?id=30247

By doing so, the file VBE6.DLL located in C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA6 will be updated to version 6.5.10.54.

5.3 Apply the patch provided with PcVue and FrontVue

As an alternative to downloading the patch directly from Microsoft, starting with the product releases listed in the Available patches section, the patch from Microsoft is shipped on the PcVue and FrontVue installation media. The patch can be found in the following folder:
\Core\Packages\Vba65\VBA65-KB2866665-x85-ENU.exe
Apply this patch manually after the installation of PcVue or FrontVue.

By doing so, the file VBE6.DLL located in C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA6 will be updated to version 6.5.10.54.

Investigations show that this patch from Microsoft is distributed via regular Windows updates but it is not applied unless an affected version of Microsoft Office is detected on the host. In any other case, the patch is not installed via Windows Updates and patching must be handled specifically despite Windows Updates being activated.

6. Available patches

Component	Vulnerability	Description
Microsoft Visual Basic for Applications	Microsoft VBA RCE	Patch provided with: • PcVue 16.2.0 • PcVue 16.1.1 • PcVue 16.0.4 • PcVue 15.2.8 • FrontVue 16.2.0 • FrontVue 16.1.1 • FrontVue 15.2.8 Patch planned for: • PcVue 12.0.30 • FrontVue 12.0.30

7. Credits

ARC Informatique thanks Automations Service, Tengizchevroil and [redacted product user] for reporting and coordinated disclosure.

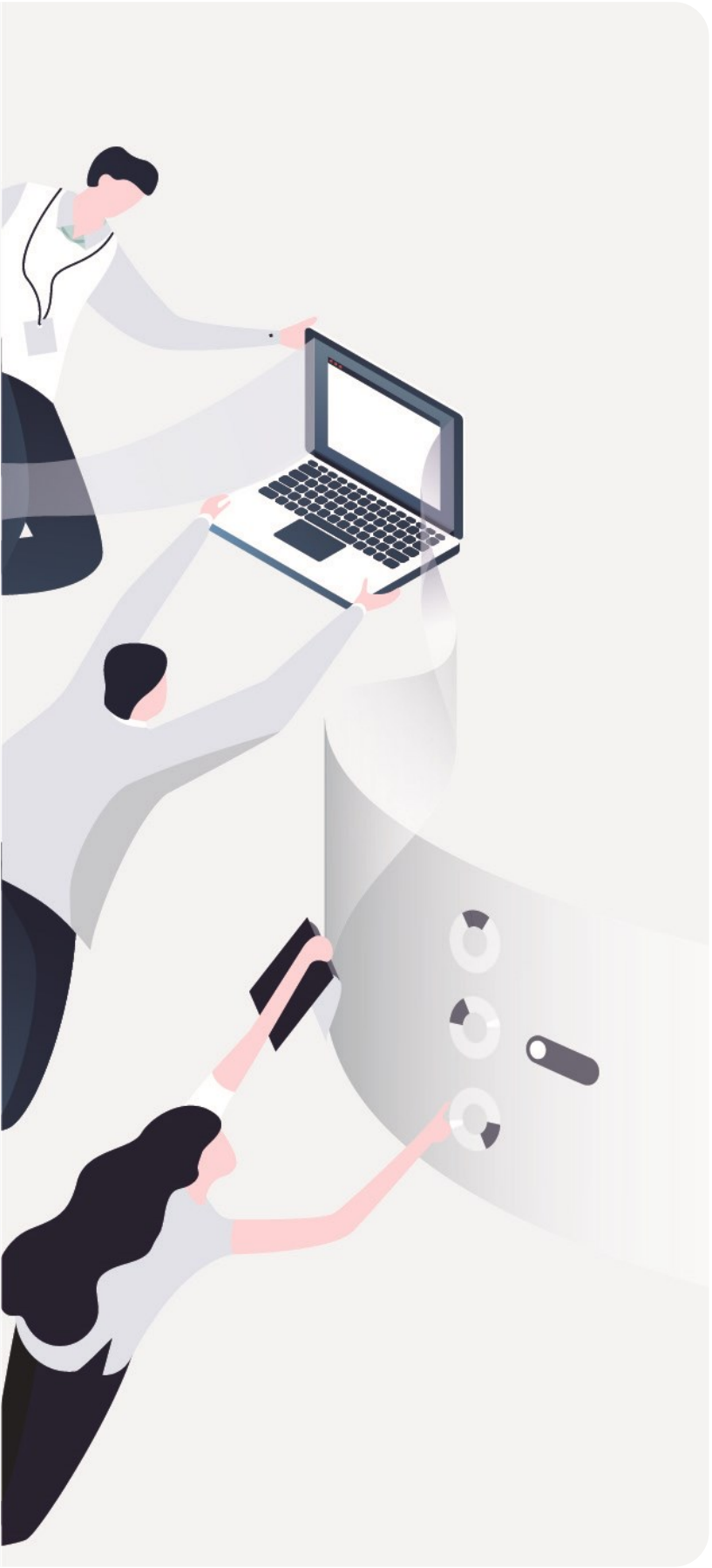
8. References

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

CVE:

- CVE-2010-0815 - MS10-031
- CVE-2012-1854 - MS12-046

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



SECURITY BULLETIN

2023-2

ARC Informatique
Private limited company
capitalized at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C / SIREN 320 695 356
VAT N°FR 19320695 356

Headquarters
2 avenue de la Cristallerie,
92310 Sèvres, France
Tél: +33 1 41 14 36 00
Hotline: +33 1 41 14 36 25
Email: arcnews@arcinfo.com
www.pcvue.com

ARC Informatique is
ISO 9001, ISO 14001 and
ISO 27001 certified

We would love to hear your thoughts and suggestions
so we can improve this document
Contact us at secure@arcinfo.com