ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-340-01—ARC INFORMATIQUE PCVUE MULTIPLE VULNERABILITIES

December 06, 2011

OVERVIEW

This Advisory is a follow-up to the Alert, "ICS-ALERT-11-271-01—PcVue HMI/SCADA Multiple ActiveX Vulnerabilities,"[a] that was published September 28, 2011, on the ICS-CERT web page.

ICS-CERT is aware of publicly and privately disclosed reports of four vulnerabilities in ARC Informatique's PcVue application. These vulnerabilities include:

- potential to write memory
- possible file corruption
- remote code execution
- denial of service.

Independent researcher Kuang-Chun Hung of Security Research and Service Institute Information and Communication Security Technology Center (ICST) privately identified a buffer overflow vulnerability in ARC Informatique's PcVue application.

Independent researcher Luigi Auriemma publicly disclosed four vulnerabilities along with proof-of-concept (PoC) exploit code, including the vulnerability privately disclosed by ICST, without coordination with ARC Informatique, ICS-CERT, or any other coordinating entity known to ICS-CERT.

ARC Informatique has confirmed these vulnerabilities and has released a patch to address the issue. Researcher Kuang-Chun Hung has tested the patch and validated that it resolves these vulnerabilities.

AFFECTED PRODUCTS

According to ARC Informatique the following products are affected:

- PcVue—All versions from 6.xx onward
- FrontVue—All versions
- PlantVue—All versions.

a. http://www.uscert.gov/control_systems/pdf/ICS-ALERT-11-271-01.pdf, website last accessed December 05, 2011.

IMPACT

Successful exploitation of these vulnerabilities could result in denial of service, write to memory, file corruption, or remote code execution.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

ARC Informatique is a French-based company that develops human-machine interface/supervisory control and data acquisition (HMI/SCADA) software that is used to interface with control systems.

According to ARC Informatique, PcVue is deployed across several sectors including manufacturing, building automation, chemical, banking and finance, electric utilities, and others. ARC Informatique estimates these products are used primarily in Europe but are also used in the US and around the world.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

ARBITRARY CODE EXECUTION

A malicious user can directly control the function pointer in SVUIGrd.ocx.

CVE-2011-4042[b] has been assigned to this vulnerability.

BUFFER OVERFLOW

An overly large integer value input to a particular parameter in SVUIGrd.ocx will cause a buffer overflow that will allow remote attackers to execute arbitrary code and gain the privileges equivalent to currently logged in user.

CVE-2011-4043[c] has been assigned to this vulnerability.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4042, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4043, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

DATA CORRUPTION

An attacker can use methods available in SVUIGrd.ocx to corrupt files on the targeted system.

CVE-2011-4044[d] has been assigned to this vulnerability.

BUFFER OVERFLOW

An ActiveX component in aipgctl.ocx is vulnerable to a buffer overflow causing a denial of service.

CVE-2011-4045[e] has been assigned to this vulnerability.

VULNERABILITY DETAILS

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

EXISTENCE OF EXPLOIT

Publicly released PoC code exists for these vulnerabilities.

DIFFICULTY

Crafting a working exploit for this vulnerability would require a moderate skill level. Exploiting the vulnerabilities would likely require social engineering to lure the target to the malicious site.

MITIGATION

ARC Informatique has released a patch to their customers to address these vulnerabilities. Users of vulnerable versions of ARC Informatique's PcVue should deploy the patch. For more information, please refer to the following ARC Informatique security bulletin:

www.pcvuesolutions.com/index.php?option=com_content&view=article&id=244&Itemid=257

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

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4044. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[e] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4045. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control system security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[f] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[g] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[h] for more information on social engineering attacks.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

[f] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 05, 2011.

[g] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed December 05, 2011.

[h] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed December 05, 2011.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.