ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-251-01—REALWINDEMO DLL HIJACK

September 07, 2012

OVERVIEW

Independent researcher Carlos Mario Penagos Hollmann has identified an uncontrolled search path element vulnerability, commonly referred to as a DLL hijack, in the RealFlex RealWinDemo application.

RealFlex has produced an upgrade to address this vulnerability, which Mr. Hollmann has validated, and it resolves the reported vulnerability.

AFFECTED PRODUCTS

The following RealFlex products are affected:

- RealWinDemo 2.1.12 and prior,
- RealWin 2.1.12 and prior, and
- FlexView 3.1.85 and prior.

IMPACT

Successful exploitation of this vulnerability may lead to arbitrary 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 this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

RealWinDemo is a Microsoft Windows-based human-machine interface/supervisory control and data acquisition (HMI/SCADA) software package that is used primarily for customer demonstration purposes. It can be used in small automation projects using standard protocols such as Modbus.

RealWin is used primarily as a demo product to generate sales of the RealFlex 6 SCADA product. RealWin is in production on projects in Nigeria, USA, India, Philippines, Saudi Arabia, and Mexico.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

UNCONTROLLED SEARCH PATH ELEMENT[a]

RealWinDemo uses an uncontrolled search path to find resources that could allow an unauthorized user to locate and exploit one or more locations. An unauthorized user could place a malicious DLL in a directory where it could be loaded before the valid DLL. An attacker must have access to the host file system to exploit this vulnerability. If exploited, this vulnerability could allow execution of arbitrary code.

CVE-2012-3004[b] has been assigned to this vulnerability. A CVSS V2 base score of 6.2 has also been assigned; the CVSS vector string is (AV:L/AC:H/Au:N/C:C/I:C/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not remotely exploitable and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads a malicious realwin.dll or keyhook.dll file.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Constructing a malicious DLL and placing it in an exploitable location requires only a low skill level. However, the attacker cannot exploit this vulnerability without local user access.

MITIGATION

RealFlex has produced an updated version that resolves the issue. Customers may log in to download an updated version of the following products:

[a] CWE-427 Uncontrolled Search Path Element, http://cwe.mitre.org/data/definitions/427.html, Web site last accessed September 06, 2012.

[b] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3004 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[c] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:L/Au:N/C:C/I:C/A:C), Web site last accessed September 06, 2012.

- RealWin 2.1.13,
- FlexView 3.1.86, and
- RealWinDemo 2.1.13.

  http://realflex.com/download/

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 systems 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.[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[e] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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 email messages.
2. Refer to Recognizing and Avoiding Email Scams[f] for more information on avoiding email scams.

[d] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 06, 2012.

[e] Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 06, 2012.

[f] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed September 06, 2012.

3. Refer to Avoiding Social Engineering and Phishing Attacks[g] for more information on social engineering attacks.

ICS-CERT CONTACT

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

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

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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.

[g] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed September 06, 2012.