ICS-CERT ADVISORY

ICSA-13-036-02— ECAVA INTEGRAXOR ACTIVEX BUFFER OVERFLOW

February 05, 2013

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts the Ecava IntegraXor application. Independent researcher Andrew Brooks has identified a buffer overflow vulnerability in Ecava's IntegraXor application.

Ecava has produced a patch that mitigates this vulnerability. The researcher has tested the patch to validate that it resolves this vulnerability. Exploitation of this vulnerability would allow an attacker to execute arbitrary code or cause a denial of service (DoS).

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following IntegraXor versions are affected:

- IntegraXor SCADA Server 4.00 build 4250.0 and earlier.

IMPACT

Successfully exploiting this vulnerability could lead to a DoS for the application or could allow an attacker to execute arbitrary code. This could impact multiple sectors, including critical manufacturing.

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

Ecava Sdn Bhd[a] is a Malaysia-based software development company that provides the IntegraXor SCADA product. Ecava specializes in factory and process automation solutions. IntegraXor is a suite of tools used to create and run a Web-based human-machine interface for a SCADA system.

IntegraXor is currently used in several areas of process control in 38 countries with the largest installation based in the United Kingdom, United States, Australia, Poland, Canada, and Estonia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

PE3DO32A.OCX BUFFER OVERFLOW[b]

The vulnerability originates from buffer overflows in the PE3DO32A.ocx service component and can occur in multiple locations of the module. An attacker would need to create a specially crafted Web page or file with an ActiveX component for the client to open. This could allow an attacker to cause a crash or to execute arbitrary code.

CVE-2012-4700[c] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).[d]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

a. Ecava, http://www.ecava.com/index.htm, Web site last accessed February 05, 2013.
b. CWE, http://cwe.mitre.org/data/definitions/119.html, CWE-119: Buffer Overflow, Web site last accessed February 05, 2013.
c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4700, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last accessed February 05, 2013.

DIFFICULTY

Social engineering is required to convince a user to go to a specially crafted Web page to exploit the vulnerability remotely. An attacker with a moderate skill level would be able to exploit the buffer overflow.

MITIGATION

Ecava has issued a customer notification[e] that details this vulnerability and provides mitigations to its customers.

Ecava recommends users download and install the update,[f] IntegraXor SCADA Server 4.00.4280, from their download Web site. The vendor also recommends that users disable ActiveX on systems where the application is being used.

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.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[g] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

e. Ecava Customer Notification, http://www.integraxor.com/blog/security-issue-for-activex-enabled-browser-vulnerability-note, Web site last accessed February 05, 2013.

f. Ecava IntegraXor 4.00.4280, http://www.integraxor.com/download.htm, Web site last accessed February 05, 2013.

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed February 05, 2013.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Mitigation Strategies,[h] 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[i] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[j] 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@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security 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.

h. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://ics-cert.us-cert.gov/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed February 05, 2013.

i. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed February 05, 2013.

j. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed February 05, 2013.

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.