ICS-CERT ADVISORY

ICSA-12-083-01—ECAVA INTEGRAXOR ACTIVEX DIRECTORY TRAVERSAL

March 23, 2012

OVERVIEW

Independent researchers Billy Rios and Terry McCorkle have identified a Path Traversal vulnerability in the Ecava IntegraXor application. Ecava has produced an update that mitigates this vulnerability. The researchers have validated that the patch fixes this vulnerability.

AFFECTED PRODUCTS

According to Ecava, the following products are affected:

- IntegraXor versions older than Version 3.71.4200

IMPACT

Successful exploitation of this vulnerability may result in file manipulation or 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

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.

a. Ecava, http://www.ecava.com/index htm, website accessed March 20, 2012.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A path traversal vulnerability[b] can occur when a specially crafted HTML document is opened on the Ecava IntegraXor server. Successful exploitation could allow file manipulation or arbitrary code execution. This vulnerability is only exploitable while using Internet Explorer due to the proprietary Active X component. No other web browsers are affected by this vulnerability

CVE-2012-0246[c] has been assigned to this vulnerability. A CVSS V2 base score of 4.3 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability requires a medium skill level. Social engineering is required to convince the user to accept the malformed HTML file.

MITIGATION

Ecava recommends users to download and install update from their website:

http://www.integraxor.com/download.htm

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.

b. http://cwe mitre.org/data/definitions/35 html, website last accessed March 20, 2012.
c. http://web nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-0246, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

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.

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*[e] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[f] 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

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.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed March 20, 2012.
e. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed March 20, 2012.
f. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed March 20, 2012.