ICS-CERT ADVISORY

ICSA-11-147-01A—ECAVA INTEGRAXOR DLL HIJACKING

UPDATE A

May 27, 2011

OVERVIEW

This advisory is a follow-up to ICS-ALERT-10-362-01—Ecava IntegraXor available at http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-10-362-01.pdf.

ICS-CERT has become aware of a Uncontrolled Search Path Element vulnerability, commonly referred to as DLL Hijacking, in the Ecava IntegraXor supervisory control and data acquisition (SCADA) product. ICS-CERT has worked with Ecava to validate the vulnerability.

Ecava has developed a patch release for IntegraXor to address this vulnerability. ICS-CERT has validated the patch.

AFFECTED PRODUCTS

This vulnerability affects all IntegraXor versions prior to Version 3.60 (Build 4090).

IMPACT

A successful exploit of this vulnerability leads to arbitrary code execution. The 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 May 25, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IntegraXor is vulnerable to DLL Hijacking.[b] An attacker may place a malicious DLL in a directory that is loaded before the valid DLL. An attacker must have access to the computer's file system to exploit this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker equires access to the computer's file system.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker requires a moderate skill level to exploit this vulnerability.

MITIGATION

ICS-CERT recommends that users of Ecava IntegraXor take the following mitigation steps:

- Update IntegraXor to the latest version and install the latest patch 3.60 (Build 4090).

  Ecava has developed and released a patch to mitigate the vulnerability

  --------- Begin Update A Part 1 of 1 ----------

  (http://www.integraxor.com/download/rc.msi).

  --------- End Update A Part 1 of 1 ----------

  For more information, customers can contact Ecava support at support@integraxor.com. Ecava's security notes can be found at http://www.integraxor.com/blog/category/security.

ICS-CERT encourages asset owners to 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 VPN, recognizing that VPN is only as secure as the connected devices.

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.

b. MITRE, http://cwe.mitre.org/data/definitions/427.html, website accessed May 24, 2011

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

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.*[c]

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.

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website accessed March 3, 2011.