ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

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

UPDATE B

June 02, 2011

OVERVIEW

This advisory is a follow up to ICSA-11-147-01A, available at: http://www.us-cert.gov/control_systems/pdf/ICSA-11-147-01A.pdf. This updated advisory addresses the possibility of remote exploit execution and provides the new URL location for the latest patch.

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 and Ecava have validated 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 may lead 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 June 01, 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.

VULNERABILITY DETAILS

EXPLOITABILITY

--------- Begin Update B Part 1 of 2 ----------

This vulnerability may be exploitable from a remote machine. If exploited, this vulnerability may allow execution of arbitrary code.

--------- End Update B Part 1 of 2 ----------

EXISTENCE OF EXPLOIT

No publicly available exploits are known to exist for 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. The patch can be downloaded from:

  --------- Begin Update B Part 2 of 2 ----------

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

  --------- End Update B Part 2 of 2 ----------

  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

[b] MITRE, http://cwe.mitre.org/data/definitions/427.html, website accessed June 01, 2011

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. 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 June 01, 2011.