ICS-CERT ADVISORY

ICSA-10-362-01—ECAVA INTEGRAXOR DIRECTORY TRAVERSAL

December 28, 2010

OVERVIEW

ICS-CERT has become aware of a directory traversal vulnerability in the Ecava IntegraXor Human-Machine Interface (HMI) product that could allow data leakage. ICS-CERT is currently in contact with representatives of Ecava who have verified the vulnerability. Ecava has developed and released a patch to mitigate the vulnerability (igsetup-3.6.4000.1.msi or later) and has notified its customer base of the availability of the patch (http://www.integraxor.com/download/igsetup.msi). This patch has been verified by both the ICS-CERT and the independent security researcher.

AFFECTED PRODUCTS

This vulnerability affects all IntegraXor versions prior to Version 3.6 (Build 4000.0). For more information, customers can contact Ecava support at support@integraxor.com.

IMPACT

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

While a successful exploit of this vulnerability could lead to arbitrary data leakage, 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 environment, architecture, and product implementation.

BACKGROUND

Ecava Sdn Bhd[a] is a Malaysia-based software development company that provides the IntegraXor product. Ecava specializes in factory and process automation solutions.

IntegraXor is a suite of tools used to create and run a web-based HMI interface for a Supervisory Control and Data Acquisition (SCADA) system.

a. Ecava, http://www.ecava.com/index htm, web page last accessed November 16, 2010.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IntegraXor is vulnerable to a directory traversal exploit. An attacker may add an arbitrary path and file and read any arbitrary file.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from a remote machine.

EXISTENCE OF EXPLOIT

This exploit is publicly known and available.

DIFFICULTY

A low level of skill is needed 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.

  Ecava has developed and released a patch to mitigate the vulnerability (http://www.integraxor.com/download/igsetup.msi). For more information, customers can contact Ecava support at support@integraxor.com.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Control system networks and remote devices should be located behind firewalls and be isolated from the business network. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be used.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[b]

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 Control System Security Program 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.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html.