ICS-CERT ADVISORY

ICSA-11-082-01—ECAVA INTEGRAXOR UNAUTHENTICATED SQL VULNERABILITY

March 23, 2011

OVERVIEW

ICS-CERT has received a report from independent security researcher Dan Rosenberg with Virtual Security Research (VSR) of an unauthenticated Structured Query Language (SQL) vulnerability in the Ecava IntegraXor human machine interface (HMI) product that could allow data leakage, data manipulation, and remote code execution against the backend host running the database service. ICS-CERT has coordinated with Ecava, which has verified the vulnerability and developed a patched release of IntegraXor (Build 4050) to address this vulnerability. Both ICS-CERT and the independent security researcher have validated the patch.

AFFECTED PRODUCTS

This vulnerability affects all IntegraXor versions prior to Version 3.60 (Build 4032).

IMPACT

A successful exploit of this vulnerability could lead to arbitrary data leakage, data manipulation, and remote code execution. The exact 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 produces 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 Supervisory Control and Data Acquisition (SCADA) systems.

IntegraXor is deployed in several areas of process control in 38 countries around the world with the largest installed base in the United Kingdom, United States, Australia, Poland, Canada, and Estonia.

a. Ecava, http://www.ecava.com/index.htm, web page accessed January 13, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IntegraXor is vulnerable to the execution of an unauthenticated SQL statement. An attacker may execute arbitrary SQL statements against the IntegraXor database by sending a specially crafted HTTP POST request. Exploitation of this vulnerability results in potential data leakage, data manipulation, and remote code execution against the backend host running the database service.

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker could exploit this vulnerability from a remote machine.

EXISTENCE OF EXPLOIT

No known publicly available exploit exists.

DIFFICULTY

An attacker would need a moderate skill level to exploit this vulnerability.

MITIGATION

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

- Use the following link to obtain the patched version of Ecava IntegraXor (Build 4050):

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

  For more information, customers should contact Ecava support at support@integraxor.com.
- 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. If remote access is required, employ secure methods such as Virtual Private Networks (VPNs).

Organizations that observe 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 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.