ICS-CERT ADVISORY

ICSA-10-322-01 — ECAVA INTEGRAXOR BUFFER OVERFLOW

December 15, 2010

OVERVIEW

The ICS-CERT has received a report from independent security researcher Jeremy Brown that reveals a stack-based buffer overflow vulnerability in the Ecava IntegraXor Human-Machine Interface (HMI) product that could allow the execution of arbitrary code. Ecava has verified the claim and has released a patch to mitigate the vulnerability (igsetup-3.5.3900.10.msi or later).

AFFECTED PRODUCTS

This vulnerability affects all IntegraXor versions prior to v3.5 (Build 3900.10). Ecava has developed a patch to mitigate this vulnerability. For more information, customers can review the Ecava announcement at http://www.integraxor.com/blog/integraxor-3-5-scada-security-issue-20101006-0109-vulnerability-note.

IMPACT

IntegraXor is currently used in several areas of process control, though primarily in Malaysia.

While a successful exploit of this vulnerability could 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 environment, architecture, and product implementation.

BACKGROUND

Ecava Sdn Bhd 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. IntergraXor is used primarily in Malaysia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IntegraXor is vulnerable to a stack-based buffer overflow when more than 1024 bytes are written to the fixed-size stack buffer. When an exploit sends a request greater than 1024 bytes, IntegraXor writes past the buffer bounds and corrupts memory, allowing execution of arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from a remote machine. No user interaction is required for an attacker to overwrite the buffer.

EXISTENCE OF EXPLOIT

There are currently no known exploits specifically targeting this vulnerability.

DIFFICULTY

Without access to exploit code similar to the test code developed by the researcher, an attacker would need at least an intermediate 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.

  The patch is available here:

  http://www.integraxor.com/download/igsetup-3.5.3900.10.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 utilized.

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 web site. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.* [1]

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.

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