ICS-CERT ADVISORY

ICSA-11-147-02—ECAVA INTEGRAXOR XSS

May 27, 2011

OVERVIEW

ICS-CERT received a report from an anonymous security reseacher concerning several cross site scripting (XSS) vulnerabilities in the Ecava IntegraXor SCADA product. ICS-CERT has worked with the reseacher and Ecava to validate these vulnerabilities.

Ecava has developed a patch release of IntegraXor to address these vulnerabilities. The independent security reseacher has validated this patch.

AFFECTED PRODUCTS

These vulnerabilites affect all IntegraXor versions prior to Version 3.60 (Build 4080).

IMPACT

A successful exploit of this vulnerability can 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 operational 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 human-machine interface for a supervisory control and data acquisition (SCADA) system.

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

[a] Ecava, http://www.ecava.com/index.htm, web page last accessed May 25, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IntegraXor is vulnerable to a reflective (nonpersistent) Cross Site Scripting[b] vulnerability. An attacker may craft a custom URL that executes an arbitrary script. Using this vulnerability, an attacker injects malicious code directly into the user's browsing session. Parameters are passed back to the user without being properly sanitized.

VULNERABILITY DETAILS

EXPLOITABILITY

Successful exploit of this vulnerability requires interaction by the user making the request. Modern web browsers have protection mechanisms against such attacks making this exploit more difficult to execute.

EXISTENCE OF EXPLOIT

Tools are publicly available that aid in exploiting this cross-site scripting vulnerability.

DIFFICULTY

An attacker needs 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 4080).

  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. 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 Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

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.

[b] MITRE, http://cwe.mitre.org/data/definitions/80.html, web page last accessed May 24, 2011

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control Systems Security Program (CSSP) 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.*[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.