ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-056-01A—PROGEA MOVICON TCPUPLOADSERVER

UPDATE A

June 14, 2011

OVERVIEW

ICS-CERT has received a report from independent security researcher Jeremy Brown of a data leakage and denial-of-service vulnerability in Progea's Movicon 11 human-machine interface (HMI) product. Progea has verified the vulnerability and has developed a patch to address the issue. ICS-CERT has verified that the patch resolves the vulnerability.

AFFECTED PRODUCTS

This vulnerability affects versions of Movicon 11.2 prior to Build 1084.

IMPACT

Movicon 11.2 is used primarily in Italy with a small percentage of installations in other European countries.

A successful exploit of this vulnerability could result in data leakage, data manipulation, or denial of service. 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

Progea Srl[a] is a privately owned Italian company.

Movicon 11 is a completely XML-based HMI development solution that includes drivers for all major Programmable Logic Controllers (PLCs). Movicon provides OPC-based connectivity for data transfer, including OPC DA and OPC XML DA services. Movicon is an XML-based HMI system that uses a web-enabled architecture based on JAVA.

[a] Progea, http://www.progea.com/, webpage last accessed February 17, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A vulnerability in TCPUploadServer.exe allows a remote, unauthenticated host to execute functions on the server. Exploiting this vulnerability will allow an attacker to delete arbitrary files, execute a program with an arbitrary argument, crash the server, obtain information about specific aspects of the remote host, and more.

An attacker can send a specially crafted packet to the server on Port 10651/TCP that can cause the system to respond with OS version and drive information. In addition, an attacker can send a specially crafted packet that causes the system to delete a file or that crashes the server.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from a remote machine.

EXISTENCE OF EXPLOIT

--------- Begin Update A Part 1 of 1 ----------

Known exploits are now targeting this vulnerability. ICS-CERT strongly urges existing users to update vulnerable installations as soon as possible.

--------- End Update A Part 1 of 1 ----------

DIFFICULTY

Crafting a working exploit for this vulnerability requires a moderate skill level. An attacker would need to reverse the packets sent between the client and server to create a crafted attack.

MITIGATION

Progea has developed and released an update to address this vulnerability: http://support.progea.com/download/Mov11.2_Setup.zip.

ICS-CERT recommends that Movicon users implement the following additional mitigation steps:

1. Implement firewall rules to limit network access to the Movicon system on Port 10651/TCP.
2. Update Movicon to the latest Version 11.2.
3. 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 isolated from the business network. If remote access is required, employ secure methods such as Virtual Private Networks (VPNs).

For more information, customers can contact Progea support at support@progea.com.

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 Systems 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.

All comments or questions related to this document should be directed to the ICS-CERT at ics-cert@dhs.gov.

[b] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, accessed February 24, 2011.