ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-131-01—PROGEA MOVICON MEMORY CORRUPTION VULNERABILITY

May 10, 2012

OVERVIEW

Security researcher Dillon Beresford of IXIA[a] has identified a memory corruption vulnerability in the Progea Movicon application. This vulnerability can be exploited by a remote attacker; however, no public exploits are currently known to exist.

ICS-CERT has coordinated these vulnerabilities with Progea, which has produced a new version (V11.3) that resolves the reported vulnerability. Mr. Beresford has tested the new version and confirms that it resolves the vulnerability.

AFFECTED PRODUCTS

Progea reports that the following products are affected:

- Movicon versions prior to 11.3.

IMPACT

An attacker can cause the server to read an invalid memory address resulting in a denial of service.

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

Progea Srl[b] is an Italian company that offers SCADA products that are deployed primarily in Europe, India, and the United States. They are used in energy, water, critical manufacturing, and several other industry sectors.

Movicon 11 is an XML-based human-machine interface development system that includes drivers for programmable logic controllers (PLCs). Movicon provides OPC-based connectivity for data transfer, including OPC DA and OPC XML DA services.

[a] http://www.ixiacom.com/, website last accessed May 10, 2012.

[b] http://www.progea.com/, website last accessed May 10, 2012.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

MEMORY CORRUPTION VULNERABILTIY[c]

Movicon is affected by an out-of-bounds read vulnerability that can be exploited by sending a specially crafted HTTP POST request to the Movicon OPC server (default Port 9090/TCP). The request will result in a denial of service.

CVE-2012-1804[d] has been assigned to this vulnerability. A CVSS V2 base score of 7.8 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a medium skill level would be able to exploit these vulnerabilities.

MITIGATION

To resolve this issue, Progea recommends installing the new version of Movicon. Users can download the new version at http://www.progea.com/en-us/downloads/programs.aspx; registration is required to access the new version.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- 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.

[c] http://cwe.mitre.org/data/definitions/119.html, this website was last accessed May 10, 2012.

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1804. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.”

- 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.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[e] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing 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 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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

[e] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed May 10, 2012.