ICS-CERT ADVISORY

ICSA-11-294-01—PROGEA MOVICON POWERHMI

October 21, 2011

OVERVIEW

This advisory is a follow-up to the Alert titled "ICS-ALERT-11-256-01 – Multiple Vulnerabilities in Progea Movicon" that was published September 13, 2011, on the ICS-CERT web page.

Two buffer overflow and one memory corruption vulnerability were disclosed affecting the Progea Movicon's PowerHMI product.

ICS-CERT has coordinated these vulnerabilities with Progea and they have produced a hotfix that mitigates these vulnerabilities.

AFFECTED PRODUCTS

The following products are affected:

- Progea Movicon 11.2.1085.3 and earlier.
- Progea Movicon PowerHMI 11.2.1085 and earlier.

IMPACT

Each of these vulnerabilities can be remotely exploitable to cause denial of service, system crash, or execution of arbitrary code.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

BACKGROUND

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

a. http://www.progea.com/, website last accessed October 20, 2011

Movicon 11 is an XML-based HMI 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.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW

A heap-based buffer overflow allows remote attackers to use an HTTP request on Port 808/TCP to cause a denial of service and possibly execute arbitrary code via a negative content-length field. CVE-2011-3491[b]has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has also been assigned.

BUFFER OVERFLOW

A heap-based buffer overflow allows remote attackers to use an HTTP request on Port 808/TCP to cause a denial of service and possibly execute arbitrary code via a long request. CVE-2011-3498[c] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has also been assigned.

MEMORY CORRUPTION

This vulnerability allows remote attackers using a Port 808/TCP HTTP request and Port 12233/TCP EIDP protocol to cause a denial of service and possibly execute arbitrary code via an EIDP packet with a large size field, which writes a zero byte to an arbitrary memory location. CVE-2011-3499[d] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploit(s) are known to target these vulnerabilities.

b http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3491 , website last accessed October 20, 2011
c http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3498 , website last accessed October 20, 2011
d http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3499 , website last accessed October 20, 2011

DIFFICULTY

An attacker with a low skill level can create a denial of service attack but a skilled attacker would be able to execute arbitrary code.

MITIGATION

Progea has developed and released a hotfix to address this vulnerability.

The hotfix can be found at the following URL:
http://support.progea.com/download/HotFix_Movicon11.2.1085.4.zip

Contact the Progea support group for instructions to aid in the installation of the hotfix:
http://www.progea.com/supporto-progea/supporto/progea-support.html

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.
- 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 system 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

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed October 20, 2011.

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 provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. 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 (ICSs) and the public at avoidable risk.