ICS-CERT ALERT

ICS-ALERT-12-137-01—PRO-FACE PRO-SERVER EX MULTIPLE VULNERABILITIES

May 16, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities affecting Pro-face Pro-Server, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. The vulnerabilities include invalid memory access, buffer overflow, unhandled exception, and memory corruption, with proof-of-concept (PoC) exploit code According to this report, these vulnerabilities are exploitable via specially crafted packets. This report was released by researcher Luigi Auriemma on his website without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified the affected vendor of the report and has asked the vendor to confirm the vulnerability and identify mitigations. No patch is currently available for these vulnerabilities.

This ICS-CERT alert provides early notice of the report and identifies baseline mitigations for reducing risks to these and other cybersecurity attacks.

The report included vulnerability details and PoC exploit code for the following vulnerability:

Vulnerability Type	Exploitable	Impact
Invalid Memory Access	Can be exploited remotely	Denial of Service / Possible Remote Code Execution
Integer Overflow	Can be exploited remotely	Denial of Service / Possible Remote Code Execution
Unhandled Exception	Can be exploited remotely	Denial of Service / Possible Remote Code Execution
Memory Corruptions	Can be exploited remotely	Denial of Service / Possible Remote Code Execution

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

Pro-face is a North American company that creates hardware and software products found in industrial, oil and gas, food and beverage, and water and wastewater industries. According to their Web site, Pro-Server EX is a data management server that collects information generated by a SCADA system and generates reports.

MITIGATION

ICS-CERT is attempting to coordinate with the vendor and security researcher to identify mitigations.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[a]
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) 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.[b]

Organizations that observe 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

ICS-CERT Operations Center
1-877-776-7585
Email: ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed May 16, 2012.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed May 16, 2012.

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats 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.