ICS-CERT ALERT

ICS-ALERT-11-271-01—PCVUE HMI/SCADA MULTIPLE ACTIVEX VULNERABILITIES

September 28, 2011

ALERT

SUMMARY

ICS-CERT is aware of a public report of four vulnerabilities with proof-of-concept (PoC) exploit code affecting the PcVue HMI/SCADA Version 10.0 product. According to the report, these vulnerabilities are remotely exploitable by using an ActiveX component within a targeted machine. This report was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has not yet verified the vulnerabilities or PoC code but has reached out to the affected vendor to notify, confirm, and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing these and other cybersecurity risks.

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

Vulnerability Type	Exploitability	Impact
Control of a function pointer	Remote	Denial of Service / Possible Remote Code Execution
Arbitrary Memory Write	Remote	Potential to Write Memory
Directory Traversal	Remote	Possible File Corruption
Array Overflow	Remote	Denial of Service/Potential Remote Code Execution

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

MITIGATION

ICS-CERT is currently coordinating with the vendor to identify useful 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 System 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]

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
ICS-CERT@DHS.GOV

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

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.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed September 28, 2011.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 28, 2011.