Important security notification – Third Party Imbedded Run-time System (ICS-ALERT-12-097-02A)

January 2013

Schneider Electric® has been made aware of a security vulnerability in the runtime logic of specific Schneider Electric PLC control systems that may be imbedded in some of its control offer.

Exploitation of this particular vulnerability could conceivably afford unauthorized individuals or parties access to privileged user functions available in the affected controllers. This includes, but may not be limited to, such functions as file transfer, read and write data to and from the controller, and the stop or start, or other state changes of the controller.

No matter what the possibility may be that such exploitation would be attempted with your control system, unauthenticated access to these control functions conceivably could, and therefore may, include an incalculable loss of system integrity, confidentiality, intellectual property and/or the availability of your control system.

On-going testing and analysis at Schneider Electric confirm that a vulnerability as indicated by this Alert exists in the third party, Version 2.x-based Runtime System supplied with some of the Schneider Electric legacy control offers (please see the list of related products later in this notice).

Schneider Electric takes these vulnerabilities very seriously and we are working closely with our vendors to investigate this alleged security vulnerability and to resolve any significant issues. Schneider Electric assures that neither customer claim nor any known exploitation of a customer machine automation system has been reported concerning Schneider Electric equipment and this particular Alert.

Details on Products Affected

The Version 2 runtime system is likely contained in the following control platforms furnished by Schneider:

- PacDrive M
- LMC 10/20
- BLC3
- BLM3
- BLS
- TLM
- TLC
- TLCC
- ATV-CI
- SMC
- Altivar ATV-IC

Schneider Electric continues to conduct research and testing to determine whether other products are affected, and will update this report with any new findings.

If you are unsure of whether you could be affected by this vulnerability or if you have any questions on this issue please contact your local Schneider Electric support center.

Risk Factors

Cyber security is a system level concern. Schneider Electric supports the Defense-in-Depth approach, and offers a large range of products to support abatement strategies that help reduce the likelihood of a cyber security event.

Only the user or system designer can be aware of all the conditions and factors that should determine your security policies, and determine the related measures required to reduce the vulnerability of your automation system. With an appropriate level of risk assessment, security planning and policy application, the materialization of the current vulnerability of the Version 2 runtime system is consequentially and effectively managed.

For more information about abatement strategies and application, please read the Schneider Electric “**How can I … Reduce Vulnerability to Cyber Attacks**” System Technical Note:

http://download.schneider-electric.com/files?p_File_Id=25779912&p_File_Name=Cyber-Security-STN-v2-Aug-2012.pdf

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a "Defense-in-Depth" approach to secure an Industrial Control System. This approach places the controllers behind one or more firewalls to restrict access to authorized personnel and protocols only.

⚠ WARNING

UNAUTHENTICATED ACCESS AND SUBSEQUENT UNAUTHORIZED MACHINE OPERATION

- Evaluate whether your environment or your machines are connected to your critical infrastructure and, if so, take appropriate steps in terms of prevention, based on Defense-in-Depth, before connecting the automation system to any network.
- Limit the number of devices connected to a network to the minimum necessary.
- Isolate your industrial network from other networks inside your company.
- Protect any network against unintended access by using firewalls, VPN, or other, proven security measures.
- Monitor activities within your systems.
- Prevent subject devices from direct access or direct link by unauthorized parties or unauthenticated actions.
- Prepare a recovery plan including backup of your system and process information.

Failure to follow these instructions can cause death, serious injury or equipment damage.