Important Security Notification – Schneider-Electric

Schneider Electric Accutech Manager RFManagerService SQL Injection

December 18, 2013

Schneider Electric® has has become aware of and has released a fix for a vulnerability involving the Accutech Manager configuration software.

The vulnerability identified:

The Accutech Manager remote host is affected by a SQL injection vulnerability.

By sending a specially crafted packet to the RFManagerService listening on port 2536 an attacker will be able to authenticate to the service and then manipulate the software.

There is no evidence that this vulnerability has been exploited in a production environment.

Message from Schneider Electric:

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address the issue. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Details on Products Affected

The following supported software versions are affected by the Accutech Manager vulnerability:

- All versions prior to V2.00.4

Details on workarounds or planned fix dates for above described Vulnerability:

Schneider Electric has fixed this issue in the latest released software version of Accutech Manager 2.00.4

Please contact your local Schneider Electric office for latest software version for Accutech Manager; alternatively this new version is available for direct download from the Schneider Electric website - http://www.schneider-electric.com/products/ww/en/6000-telemetry-remote-scada-systems/6050-wireless-instrumentation/61237-accutech/?BUSINESS=1

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.

Download our Cyber Security whitepaper from www.schneider-electic.com.

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system they should be adapted by individual users as required.

For the CVSS cognoscenti, the vector is: N/AC:L/Au:N/C:C/I:C/A:C

CVSS Base Score: 10.0