Important Security notification – Accutech Manager Software tool

February 5, 2013

Schneider Electric® has become aware of a vulnerability in the Accutech Manager software tool.

The vulnerability identified is:

(1) Accutech Manager

> A software crash or potential code execution exploit, caused by a heap overflow, can occur if a GET message exceeding 260 bytes is sent to TCP port 2537

This vulnerability would require network access to the PC running the software tool, at the time the software tool is operating.

This vulnerability was discovered during cyber-security research both by an external researcher and by Schneider Electric internal investigations. We have no evidence that this vulnerability has been exploited.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. 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 products are affected

Accutech Manager

Accutech Manager Version 2.00.1 and older may have this vulnerability. Upgrading to a later version fixes this vulnerability.

Details on workarounds and planned fix dates for above described Vulnerabilities

1) Ability to crash Accutech Manager Software

Schneider Electric will fix this issue in the next maintenance revision of Accutech Manager, planned for February 28, 2013.

Exposure of this vulnerability can be reduced by closing the Accutech Manager Software tool's server component when it is not in use.

Please contact your local Schneider Electric office for latest software for Accutech range of products.

If a fix is not yet available or it is not possible to apply the new software to an existing installation at this time, then Schneider Electric has produced general recommendations (see below). Please contact your local Schneider Electric office for more information.

2) General Recommendations

Schneider Electric has been designing industrial automation products for many years 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 PLCs behind one or more firewalls to restrict access to authorized personnel and protocols only. The location of the firewalls is decided based on how large the trusted zone is required to be. Please see our website for more detailed information:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

Or navigate from our web site: **www.schneider-electric.com**

Support > Cybersecurity

Acknowledgments

Schneider Electric wishes to thank researcher Aaron Portnoy, Exodus Intelligence for reporting of the vulnerability and working with Schneider Electric during the disclosure process

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.

(1) Ability to crash Accutech Manager software or execute unintended code as a result of using a GET message

CVSS Base Score: 10

(AV:N/AC:L/Au:N/C:C/I:C/A:C)