The CERT for France Industry, Services and Tertiary sector

Vulnerability in Schneider Electric Accutech Manager (SCADA)

Reference : CERT-IST/AV-2013.128
Version : 1.0
Version date : 13 February 2013

Vulnerability classification

Risk : Very high
Impact : Take control
Attack expertise : Skilled
Attack requirements : Remote (no account) over an exotic service

System Information

Affected Platform(s) :

- Microsoft Windows systems

Affected Software :

- Accutech Manager versions 2.00.1 and prior

Exhaustive list of affected products in the Cert-IST catalog :

Description

Publication context :

This vulnerability had the**FA-2013.0023**reference in the Cert-IST list of flaws under investigation.

Problem description :

A vulnerability has been discovered in the Schneider Electric's Accutech Manager application. It allows a malicious person to remotely cause a denial of service or to take the full control of a vulnerable system.

Note: An exploit code for this vulnerability has been released on Internet.

Technical context :

Accutech Manager, is a management component of a network-based sensor monitoring system. Accutech Manager is used in applications where remote sensor data are gathered, monitored, displayed, and archived over time.

Technical information :

This vulnerability is due to a buffer overflow that may ocur when handling very long GET requests. It allows a remote attacker, by sending specially crafted network traffic to TCP port 2537, to crash the application or to execute arbitrary code with the administrator privileges.

Solution

Update Accutech Manager to version 2.00.2 or later

English translation not available yet

- Schneider Electric Accutech software updates
  - http://www.schneider-electric.com/download/ww/en/results/0/1555898-Software--Released/28460036-Accutech/

CVSS score(s)

- Cert-IST - CERT-IST/AV-2013.128
  - Base score : 10.0 - AV:A/AC:L/Au:N/C:C/I:C/A:C
  - Temporal score : 8.3 - AV:A/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

Standard vulnerability ID(s)

- CVE: CVE-2013-0658

Additional Resources

- Schneider Electric security advisory SEVD 2013-021-01 dated January 21, 2013
  - http://www.schneider-electric.com/download/ww/en/details/35974865-Vulnerability-Disclosure-for-Accutech-Manager-SW/
- ICS-CERT security advisory ICSA-13-043-01 dated February 12, 2013
  - http://ics-cert.us-cert.gov/pdf/ICSA-13-043-01.pdf

Version	Comment	Date
1.0	Advisory creation	13/02/2013