ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-043-01—SCHNEIDER ELECTRIC ACCUTECH MANAGER HEAP OVERFLOW

February 12, 2013

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts the Schneider Electric Accutech Manager.

Independent researcher Aaron Portnoy of Exodus Intelligence[a] has identified a heap-based buffer overflow vulnerability in Schneider Electric's Accutech Manager application. Schneider Electric has produced an update that mitigates this vulnerability. This researcher has tested the update and verified that it fixes the vulnerability. Exploitation of this vulnerability could allow an attacker to execute code with administrator privileges. This vulnerability could affect the energy, water and wastewater, and critical manufacturing sectors.

This vulnerability could be exploited remotely.

Exploit code for this vulnerability has recently been published by another researcher who was not part of any coordinated effort with the vendor, ICS-CERT, or Exodus Intelligence.

AFFECTED PRODUCTS

The following Schneider Electric versions are affected:

- Accutech Manager 2.00.1 and older.

IMPACT

This buffer overflow will cause the Accutech Manager application to crash and could be exploited to allow an attacker to execute arbitrary code with administrator privilege. Because this vulnerability can be exploited remotely, there is a potential for an attacker to gain control of the host computer.

[a] Exodus Intelligence - https://www.exodusintel.com/ , Web site last accessed February 12, 2013.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Schneider Electric is a Europe-based company that maintains offices in 190 countries worldwide. Their products address various markets including renewable energy, process control, monitoring and control, motor controls, lighting controls, electrical distribution, and security systems.

The affected product, 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. It can be used in a broad range of low-level applications ranging from long-term multi-sensor monitoring on a large network to single PC implementations for technicians.

According to Schneider Electric, Accutech Manager is deployed across several sectors including energy, water and wastewater, and critical manufacturing.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

HEAP-BASED BUFFER OVERFLOW[b]

The RFManagerService.exe process binds to Ports 2536/TCP and 2537/TCP by default. By sending an HTTP request outside the bounds of the buffer to Port 2537/TCP, an attacker can cause a heap-based buffer resulting in loss of confidentiality, integrity, and availability.

CVE-2013-0658[c] has been assigned to this vulnerability. ICS-CERT has assigned a base CVSS score of 10.0; the CVSS vector string is: (AV:N/AC:L/Au:N/C:C/I:C/A:C).[d]

[b] CWE, http://cwe.mitre.org/data/definitions/122.html, CWE-122: Heap-based Buffer Overflow, Web site last accessed February 12, 2013.

[c] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0658 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[d] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C) Web site last visited February 12, 2013.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploit code for this vulnerability has been recently published.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

Schneider Electric has released an update[e] that mitigates this vulnerability. The researcher has tested the update and verified that it fixes the vulnerability.

This update is available at the Schneider Electric Website:

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

Schneider Electric also recommends that users implement the following steps until the update can be applied.

- Close the Accutech Manager software tool's server component when not in use.
- Obtain guidance from Schneider Electric's cybersecurity recommendations Web page.[f]
- Check with Schneider Electric, and apply the maintenance update as soon as it becomes available.

One specific strategy that can mitigate the risk associated with the vulnerability is to ensure that the vulnerable port (2537/TCP) is not accessible from the Internet.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.

[e] Schneider Electric Download Link, http://www.schneider-electric.com/download/ww/en/results/0/1555898-Software--Released/28460036-Accutech , Web site last accessed February 12, 2013.

[f] Vendor's security recommendations - http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page, Web site last accessed February 12, 2013.

- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[g] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Mitigation Strategies,[h] available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing 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

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

[g] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed February 12, 2013.

[h] Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed February 12, 2013.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.