ICS-CERT ADVISORY

ICSA-11-285-01—HONEYWELL TEMA REMOTE INSTALLER ACTIVEX VULNERABILITY

October 12, 2011

OVERVIEW

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received a report from independent security researchers Billy Rios and Terry McCorkle concerning a vulnerability affecting Honeywell Enterprise Buildings Integrator (EBI) software systems that have Temaline physical access control products installed. Temaline client products use the Tema Remote Installer to download and install required Tema components for client workstation access.

Tema Remote Installer uses DownloadURL() ActiveX function configured to ignore file authentication. This misuse of an ActiveX function allows download and installation of any MSI file without checking source authenticity or user notification.

ICS-CERT has coordinated this vulnerability report with Honeywell and the researchers. Honeywell has released two patches resolving this vulnerability. ICS-CERT has validated that these patches resolve the reported vulnerability.

AFFECTED PRODUCTS

According to Honeywell, the following EBI product versions are affected:

- EBI R310.1 - TEMA 4.8
- EBI R310.1 - TEMA 4.9
- EBI R310.1 - TEMA 4.10
- EBI R400.2 SP1 - TEMA 5.2
- EBI R410.1 - TEMA 5.3.0
- EBI R410.2 - TEMA 5.3.1.

IMPACT

Successful exploitation of this vulnerability may result in the ability to execute arbitrary code on the targeted human-machine interface system.

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

Honeywell EBI is a building system integration software product sold globally by Honeywell Building Solutions and Honeywell Process Solutions. Building operators and facility engineers use EBI to control HVAC, physical security, life safety and energy systems. The EBI software monitors alarms and events and allows for system configuration and administration as required.

The TEMA Remote Installer is an automated software installation tool provided by Honeywell to support installation of Temaline workstation clients.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The TEMA Remote Installer contains an ActiveX control that exposes a method that allows execution of arbitrary code. If a specially crafted MSI file renamed “ThinClient_TemaKit.msi” is downloaded using Honeywell’s TEMA Remote Installer, the file will be silently installed on the target machine. This specially crafted MSI file could then alter the functionality and control of the running EBI system and enable other unauthorized remote actions. The implementation of this ActiveX control does not verify the origin of the MSI file, allowing an attacker to craft an MSI file that can be downloaded and silently installed on the target machine.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No public exploits are known that specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would require moderate skill.

MITIGATION

Honeywell has produced a patch that resolves this vulnerability which can be acquired by contacting their regional Security Technical Consultant. Contact information is provided below. Honeywell recommends this update be applied to all systems running affected versions of the EBI system regardless of current connection status to the Internet.

ICS-CERT has confirmed the vendor patch resolves the reported vulnerability. The patched ActiveX controls do not allow the legitimate ThinClient_TemaKit.msi to be downloaded. Any future clients

requiring the ThinClient_TemaKit.msi to be installed should follow the installation instructions as specified in the update notice.

Honeywell Building Solutions (HBS) customers with impacted EBI products should contact their local service account manager to arrange for updates to be applied by HBS service technicians. The update should be applied to:

- All EBI Server computers
- All EBI client computers that have had Station Client and Temaline Web Clients installed.
- All computers that have had Temaline Web Reception installed.

Honeywell Process Solutions customers with impacted EBI products should contact their appropriate regional Industrial Security Technical Consultant from the following list:

- Pacific Region - Ajay Varghese +61 738 406493
- EMEA Region - Suresh Vijayakumar +971 56 6164177
- North America - Mike Torbett +1 713 5400408
- Latin America Region - Alejandro Giudici +54 911 59436195

In addition to applying the patch available, ICS-CERT encourages asset owners to take further defensive measures to lower their risk to the possible exploitation of this and other cybersecurity risks.

Specifically, ICS-CERT encourages asset owners to:

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

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[a]

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open unsolicited attachments in e-mail messages

a. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed October 11, 2011.

1. Refer to *Recognizing and Avoiding Email Scams* [b] for more information on avoiding e-mail scams
2. Refer to *Avoiding Social Engineering and Phishing Attacks* [c] for more information on social engineering attacks.

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:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. 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 (ICSs) and the public at avoidable risk.

b. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed October 11, 2011.

c. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed October 11, 2011.