ICS-CERT ADVISORY

ICSA-11-103-01A—HONEYWELL SCANSERVER ACTIVEX CONTROL

UPDATE A

August 15, 2011

OVERVIEW

--------- Begin Update A Part 1 of 3 ----------

This ICS-CERT Advisory is an update to ICSA-11-103-01 – Honeywell ScanServer ActiveX Control, which was originally released on April 13, 2011.

A security research company, Secunia[a], has released a report of a use-after-free vulnerability[b] in the ScanServer ActiveX control, including proof-of-concept (POC) exploit code. This report indicates that successful exploitation of this vulnerability can lead to arbitrary code execution.

When a client system accesses a web page created with the vulnerable version of Honeywell's Web Toolkit, it will receive an ActiveX component that is vulnerable to exploitation if the client system subsequently visits a malicious website.

Honeywell has confirmed this vulnerability and has released a patch to address the issue. ICS-CERT has validated Honeywell's patch.

In addition to the patch issued by Honeywell, Microsoft has issued an ActiveX killbit for the affected control. To obtain this killbit, users can download the cumulative update from Microsoft for August 2011.

--------- End Update A Part 1 of 3 ----------

AFFECTED PRODUCTS

The affected product is Honeywell's ScanServer ActiveX control, which is a component of the Web Toolkit (Version 780.0.20.5) that is packaged with all versions of Honeywell SymmetrE. Web Toolkit may also be licensed separately for use with other software products.

IMPACT

a. Secunia, http://www.secunia.com, website last accessed August 11, 2011.

b. CWE-416 Use After Free (1.12), Common Weakness Enumeration, http://cwe.mitre.org/data/definitions/416.html, website las accessed April 4, 2011.

All systems that browse to a SymmetrE or other server that contains web pages created with the vulnerable version of the Honeywell Web Toolkit are potentially impacted by this vulnerability.

BACKGROUND

Honeywell SymmetrE is a software product sold globally by Honeywell Building Solutions for building automation applications. Building operators and facility engineers use SymmetrE to control HVAC systems. The SymmetrE software monitors alarms and events in the HVAC system and allows setting schedules for managing comfort and energy use during the occupied and unoccupied periods.

Web Toolkit is a suite of tools that allows the customer's building engineers to create and publish a web page allowing building occupant control of set points for environment comfort and lighting systems. Building occupants typically use this functionality for after-hours settings.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The vulnerability is caused by a use-after-free error when handling the "addOSPLext()" method and can be exploited to dereference already freed memory via a specially crafted web page.

According to Honeywell, if the affected version of HoneyWell Web Toolkit exists in the list of currently installed programs in the Windows "Add or Remove Programs" control panel, the system should be assumed to be vulnerable.

--------- Begin Update A Part 2 of 3 ----------

Secunia has produced two advisories related to this vulnerability. These advisories can be found at the following locations:

- http://secunia.com/advisories/43360/
- http://secunia.com/secunia_research/2011-22/

--------- End Update A Part 2 of 3 ----------

VULNERABILITY DETAILS

EXPLOITABILITY

To exploit this vulnerability, an attacker would need to create a specially crafted web page, and lure a user who has the vulnerable ActiveX component installed on their client system to that malicious site.

Honeywell has provided the following risk assessment for customer sites using SymmetrE or Web Toolkit:

- Moderate—server and client machines that have Web Toolkit installed, or visiting clients that have accessed the SymmetrE web page created with Web Toolkit and have public Internet access but have not been updated as prescribed in the Mitigation section of this advisory.
- Low—SymmetrE server and client machines that have Web Toolkit installed, or visiting clients that have accessed the SymmetrE web page created with Web Toolkit but do not have access to public Internet are better protected from the vulnerability. This assumes that unrelated vulnerabilities have not subverted the segregation between intranet and the Internet. All server, workstation clients, and visiting client machines in this category should still be updated according to the information contained in the Mitigation section of this advisory.
- None—SymmetrE Server platforms with Web Toolkit licensed but not installed, and that have not created web pages with Web Toolkit for user access. Verify installation status on server and workstation clients by looking in the "Add Remove Programs" Control Panel to see if Web Toolkit is listed as an installed program. If installed, remediate by following the Mitigation section of this Advisory.

EXISTENCE OF EXPLOIT

Publicly released PoC code exists for this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would require a moderate skill level. Exploiting the vulnerability would likely require social engineering to lure the target to the malicious site.

MITIGATION

ICS-CERT recommends that users of Honeywell Web Toolkit take the following mitigation steps:

- Honeywell Environmental Combustion and Control (ECC) SymmetrE customers should use the following link to obtain the updated version of Web Toolkit ScanServer component build 862.1.10.1. Users should install this update on the SymmetrE server and workstation clients following the Software Release Bulletin instructions. Once installed, clients will receive the updated ActiveX control when they connect to the SymmetrE web page.

  The update can be found here: https://extranet.honeywell.com/ecc/TheBuildingsForum under the "XL5000 – SymmetrE" section.

  Note that access to this website requires registeration.

--------- Begin Update A Part 3 of 3 ----------

- Microsoft has issued an ActiveX killbit for the affected control. To obtain this killbit, users can download the cumulative update from Microsoft for August 2011.

--------- End Update A Part 3 of 3 ----------

- Any user who has installed and used the Web Toolkit to create a webpage for users' access should apply this update to their SymmetrE server and workstation clients, then reconnect visiting clients to obtain the updated ActiveX control on those clients as soon as possible. For more information, customers should contact Honeywell ECC support in their region.
- Honeywell Building Solutions (HBS) customers should contact their local account manager to arrange for updates to be applied by HBS service technicians onsite.

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

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 Control Systems Security Program 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.