ICS-CERT ADVISORY

ICSA-12-150-01—HONEYWELL HMIWEB BROWSER BUFFER OVERFLOW VULNERABILITY

September 07, 2012

OVERVIEW

This advisory is a follow-up to the original advisory titled ICSA-12-150-01P—Honeywell HMIWeb Browser Buffer Overflow Vulnerability that was originally posted to the US-CERT secure Portal library.

ICS-CERT received a report from Honeywell and the Zero Day Initiative (ZDI),[a] concerning a buffer overflow vulnerability in all products using the Honeywell HMIWeb browser. This vulnerability was reported to ZDI by an anonymous researcher.

Honeywell has created specific patches, based on the product version, that address this issue. These patches have not been independently validated.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The affected products and versions are:

1. Honeywell Process Solutions:
   - Experion Releases R400.x, R31x, R30x, and R2xx,
2. Honeywell Building Solutions:
   - Enterprise Building Manager Releases,
3. R400 and R410.1 and SymmetrE R410.1 release,
4. Honeywell Environmental Combustion & Controls, and
5. SymmetrE R410.1 release.

a. http://www.zerodayinitiative.com/, Web site last accessed September 06, 2012.

IMPACT

Successful exploitation of this vulnerability could allow remote, unauthenticated attackers to execute arbitrary code on a vulnerable 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 Experion PKS is a distributed control system solution sold globally by Honeywell Process Solutions. Experion PKS is used for automation and control of industrial and manufacturing processes.

Honeywell Enterprise Buildings Integrator (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.

Honeywell SymmetrE is a building system integration software product sold by Environmental and Combustion Controls in North and South America. Building operators and facility engineers use SymmetrE to primarily control HVAC systems and for open protocol integration. The SymmetrE software monitors alarms and events and allows for system configuration and administration as required.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

STACK-BASED BUFFER OVERFLOW[b]

The Honeywell HMIWeb Browser HSCDSPRenderDLL ActiveX control contains a stack buffer overflow that can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.

b. http://cwe.mitre.org/data/definitions/121.html, Web site last accessed September 06, 2012.

CVE-2012-0254[c] has been assigned to this vulnerability. A CVSS V2 base score of 3.4 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

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

MITIGATION

Honeywell Process Solutions (HPS) and Honeywell Building Solutions (HBS) have released fixes for this vulnerability.

HPS customers should download the security notification that describes the vulnerability and provides a link to the fixes at: www.honeywellprocess.com

- Select **Support**, then select **Latest Notifications** (or use this LINK).
- Open document SN 2012 03 09 01A Security Vulnerability in HMIWeb Browser.

No login is required to view the document. However, login is required to download software using links in Honeywell's SN document.

HBS customers should contact their local account manager to arrange for updates to be applied by HBS service technicians.

Honeywell Environmental Combustion and Control (ECC) SymmetrE customers or their contractors should use the URL below to obtain HMIWeb Browser update. Users should install this update on the SymmetrE server and workstation clients following the Software Release Bulletin instructions.

The update can be found here: https://extranet.honeywell.com/ecc/TheBuildingsForum under the XL5000—SymmetrE section. Access to this Web site requires registration.

c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0254 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

Additional Precautions

- Do not use a Station node to connect to the Internet for the purposes of Web browsing.
- If a Station node is connected to the Internet, do not use Station or Internet Explorer to browse the Internet, or limit this usage only to trusted Web sites.

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

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.

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

1. Do not click Web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams[e] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[f] for more information on social engineering attacks.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 06, 2012.

e. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed September 06, 2012.

ICS-CERT CONTACT

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

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP 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.

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.

f. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed September 06, 2012.