ICS-CERT ADVISORY

ICSA-13-024-01—BEIJER ELECTRONICS ADP AND H-DESIGNER BUFFER OVERFLOW VULNERABILITY

January 24, 2013

OVERVIEW

This advisory provides details about a buffer overflow vulnerability in multiple Beijer Electronics' ADP and H-designer products. Independent researcher Kuang-Chun Hung of Information and Communication Security Technology Center (ICST) has identified a buffer overflow vulnerability in Beijer ADP and H-Designer applications. This vulnerability can allow attackers to execute arbitrary code and gain unauthorized access. This vulnerability affects systems deployed in the critical manufacturing, food and agriculture, transportation, and energy sectors.

Beijer has created a new version that corrects this vulnerability. Researcher Morgan Hung has tested this version to verify that it mitigates the reported problem.

AFFECTED PRODUCTS

The following Beijer products are affected:

- ADP V6.5.0-180_R1967
- ADP V6.5.1-186_R2942
- H-Designer 6.5.0 B180_R1967

IMPACT

Successful exploitation of this vulnerability may allow an attacker the ability to execute arbitrary code and gain the privileges of the currently logged in user.

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

Beijer[a] is a Sweden-based industrial automation and data communications company that maintains offices in several countries around the world, including the US, UK, Germany, France, Taiwan, China, and Brazil.

ADP is a configuration tool used to create applications for operator terminals, and H-Designer is HMI configuration software.

According to Beijer, their products are deployed across several sectors including critical manufacturing, food and agriculture, transportation, energy, and others.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW[b]

An attacker can input a long string into a dll file used by ADP and H-Designer, which can cause a buffer overflow. This vulnerability could allow arbitrary code execution, which could affect the integrity of the system.

a. Beijer corporate Web site, http://www.beijerelectronics.com, Web site last accessed January 24, 2013.

b. CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, http://cwe.mitre.org/data/definitions/119.html, Web site last accessed January 24, 2013.

CVE-2012-4696[c] has been assigned to this vulnerability. A CVSS v2 base score of 6.9 has been assigned; the CVSS vector string is (AV:L/AC:M/Au:N/C:C/I:C/A:C).[d]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not exploitable remotely and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed dll file.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability could be difficult.

MITIGATION

Beijer Electronics created Version 6.1.1 to address this vulnerability. The researcher who originally reported the vulnerability has tested the newest version and verified that it fixes the issue. Users can obtain the latest version by contacting their local distributor.

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.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4696, 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:L/AC:M/Au:N/C:C/I:C/A:C), Web site last accessed January 24, 2013.

Strategies.[e] 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—(UPDATE) Targeted Cyber Intrusion Detection and Mitigation Strategies,[f] that is 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.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public Web sites. All comments or questions related to this document should be directed to ICS-CERT at ics-cert@hq.dhs.gov.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 24, 2013.

f. Target Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed January 24, 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.