ICS-CERT ADVISORY

ICSA-12-145-02—XARROW MULTIPLE SECURITY VULNERABILITIES

May 24, 2012

OVERVIEW

This advisory is a follow-up to ICS-ALERT-12-065-01[a] titled xArrow Multiple Vulnerabilities that was published March 05, 2012, on the ICS-CERT Web page.

Independent security researcher Luigi Auriemma identified and released four security vulnerabilities, along with proof-of-concept code, in the xArrow software application without coordination with ICS-CERT, the vendor, or any other coordinating entity. The following remotely exploitable vulnerabilities were identified:

1. NULL Pointer Dereference,
2. Heap-Based Buffer Overflow,
3. Out-of-Bounds read, and
4. Improper Restriction of Operations within the Bounds of a Memory Buffer.

xArrow has produced a new version that resolves the reported vulnerabilities. Luigi Auriemma has tested the new version and confirmed that the vulnerabilities have been resolved.

AFFECTED PRODUCTS

The following xArrow[b] versions are affected:

- xArrow software versions older than Version 3.4.1

IMPACT

Exploitation of these vulnerabilities may cause the xArrow service to crash causing a denial-of-service condition or allow an attacker to execute arbitrary code.

a. ICS-CERT ALERT, https://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-065-01.pdf, Web site accessed May 25, 2012.

b. xArrow download site, http://www.xarrow.net/download.htm, Web site accessed May 25, 2012.

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

BACKGROUND

xArrow is a human-machine interface (HMI) system. According to xArrow, this product is a general configuration software tool used to monitor and collect data primarily in industrial control, infrastructure, or facility-based processes.

xArrow Software is a software developer, located in China. xArrow is an HMI that can be used in building automation, water treatment, environmental automation framework monitoring, agricultural greenhouses monitoring, etc. xArrow systems are deployed mainly in China, India, Indonesia, Poland, and Latvia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

NULL POINTER DEREFERENCE[c]

A NULL pointer dereference occurs when the xArrow server allocates memory without checking the buffer returned by calloc(), which may cause a crash or exit.

CVE-2012-2426[d] has been assigned to this vulnerability. A CVSS v2 base score of 7.1 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N/A:C). [e]

HEAP-BASED BUFFER OVERFLOW[f]

The xArrow server stores client data without bounds checking. By sending additional valid packets, an attacker could partially control corruption to force the arbitrary freeing of a memory address. This could allow the attacker to cause a crash or to execute arbitrary code.

c. CWE, http://cwe.mitre.org/data/definitions/476.html , CWE-476: NULL Pointer Dereference, Web site last accessed May 25, 2012.
d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2426, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:N/A:C), Web site last visited May 25, 2012.
f. CWE, http://cwe.mitre.org/data/definitions/122.html, CWE-122: Heap-based Buffer Overflow, Web site last accessed May 25, 2012.

CVE-2012-2427[g] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C). [h]

OUT-OF-BOUNDS READ[i]

xArrow reads data past the end of the intended buffer. This is possible because of an integer overflow during the checking of the available packet size. This could cause corruption of sensitive information, a crash, or allow arbitrary code execution.

CVE-2012-2428[j] has been assigned to this vulnerability. A CVSS v2 base score of 8.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:P/A:C).[k]

IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER[l]

When performing operations on a memory buffer, xArrow reads data from a memory location that is outside the intended boundary of the buffer. As a result, an attacker may be able to execute arbitrary code, alter the intended control flow, read sensitive information, or cause the system to crash.

CVE-2012-2429[m] has been assigned to this vulnerability. This vulnerability has a CVSS v2 base score of 9.3[n] has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C)

g. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2427 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
h. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last visited May 25, 2012.
i. CWE, http://cwe.mitre.org/data/definitions/125.html, CWE-125: Out-of-Bounds Read, Web site last accessed May 25, 2012.
j. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2428, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
k. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:P/I:P/A:C), Web site last visited May 25, 2012.
l. CWE, http://cwe.mitre.org/data/definitions/119.html , CWE-119: Improper Restriction of Operations within the Bounds of a Memory buffer, Web site last accessed May 25, 2012.
m. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2429, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
n. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last visited May 25, 2012.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a moderate skill level would be able to exploit these vulnerabilities.

MITIGATION

xArrow has produced an updated software version (3.4.2) that resolves the reported vulnerabilities. The new version can be downloaded here: http://www.xarrow.net/download.htm.

xArrow recommends users uninstall the old version and install the new. All project data will be preserved.

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

o. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed May25, 2012.

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@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 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.