ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-059-01—ABB ROBOT COMMUNICATIONS RUNTIME BUFFER OVERFLOW VULNERABILITY

February 28, 2012

OVERVIEW

ICS-CERT received a report from ABB and the Zero Day Initiative (ZDI)[a] concerning a buffer overflow vulnerability in the Robot Communication Runtime software used to communicate with IRC5, IRC5C, and IRCP robot controllers. This vulnerability was reported to ZDI by independent security researcher Luigi Auriemma.

If exploited, this vulnerability could allow an attacker to cause a denial of service to the robot scanning and discovery service on the computer and potentially execute remote code with administrator privileges.

ABB has developed a patch to address this issue.

AFFECTED PRODUCTS

The following ABB products and versions are affected:

- ABB Interlink Module: Versions 4.6 through 4.9
- IRC5 OPC Server: Versions up to and including 5.14.01
- PC SDK: Versions up to and including 5.14.01
- PickMaster 3: Versions up to and including 3.3
- PickMaster 5: Versions up to and including 5.13
- Robot Communications Runtime: Versions up to and including 5.14.01
- RobotStudio: Versions supporting IRC5 up to and including 5.14.01
- RobView 5: *Works together with other products listed here.*
- WebWare SDK: Versions 4.6 through 4.9
- WebWare Server: Versions 4.6 through 4.91

[a] http://www.zerodayinitiative.com/, website last accessed February 27, 2012.

IMPACT

An attacker may be able to use this vulnerability to cause a denial of service for the robot scanning and discovery service and potentially execute code remotely on the Windows PC. Depending on the installation, the remote code execution could run with administrator privilege.

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

According to ABB, RobotStudio and PickMaster 5 are used in installation, programming, and commissioning of ABB industrial robots. PickMaster 3, IRC5 OPC Server, and WebWare SDK are used for continuous operations and custom human-machine interfaces for Windows PCs connected to the robot controller over a factory network.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

According to ZDI, the vulnerability exists within RobNetScanHost.exe and its parsing of network packets accepted on Port 5512/TCP. By sending a specially crafted packet, an attacker can cause the RobNetScanHost service to terminate, resulting in a denial of service that prevents robot controllers from being discovered on the network. An attacker may be able to use the buffer overflow to download and execute code on the affected PC.

BUFFER OVERFLOW[b]

The vulnerability originates from a buffer overflow in the RobNetScanHost service component when processing incoming announcements of robot controller availability on the network.

CVE-2012-0245[c] has been assigned to this vulnerability. A CVSS V2 base score of 10 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

[b] http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0245, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill level would be able to exploit the buffer overflow while more advanced knowledge would be required to execute arbitrary code.

MITIGATION

ABB has issued a customer notification as well as a patch to correct this vulnerability which can be found here:

http://www05.abb.com/global/scot/scot348.nsf/veritydisplay/f261be074480dc24c12579a00049ecd5/$file/si10227a1%20vulnerability%20security%20advisory.pdf

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 with properly configured rules addressing Port 5512/TCP, 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.

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

[d] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed February 27, 2012.

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.