ICS-CERT ALERT

ICS-ALERT-11-256-05A—ROCKWELL RSLOGIX OVERFLOW VULNERABILITY

September 19, 2011

ALERT

SUMMARY

This Alert Update is a follow-up to the original ICS-CERT Alert titled "ICS-ALERT-11-256-05—ROCKWELL RSLOGIX OVERFLOW VULNERABILITY" that was published September 13, 2011, on the ICS-CERT web page.

ICS-CERT is aware of a public report of an overflow vulnerability with proof-of-concept (POC) exploit code affecting the Rockwell RSLogix 5000, Version 19. According to this report, services running on Port 4446 are vulnerable to a memory overflow. This report was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has not yet verified the vulnerabilities or POC code, but has reached out to the affected vendor to notify, confirm, and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

----- UPDATE 1 of 3 -----

Rockwell has released the following advisories:
Security Advisory Index: http://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102

FactoryTalk RnaUtility.dll Vulnerability September 16, 2011, Advisory:
http://rockwellautomation.custhelp.com/app/answers/detail/a_id/456144

----- END UPDATE 1 of 3 -----

The report included vulnerability details and POC exploit code for the following vulnerability:

Vulnerability Type	Exploitability	Impact
Overflow	Remote	Denial of Service

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

BACKGROUND

Rockwell Automation provides industrial automation control and information products worldwide, across a wide range of industries.

The Rockwell RSLogix family is a group of ladder logic programming packages that operates on Microsoft Windows operating systems.

----- UPDATE 2 of 3 -----

RSLogix 5000 supports the Allen-Bradley ControlLogix and GuardLogix family of programmable controllers.

----- END UPDATE 2 of 3 -----

MITIGATION

----- UPDATE 3 of 3 -----

Rockwell Automation is aware of this vulnerability and plans to release a software patch within 14 days. Rockwell recommends configuring firewalls to block the following TCP ports to prevent traversal of RNA messages in and out of the ICS system:

- 1330
- 1331
- 1332
- 4241
- 4242
- 4446
- 6543
- 9111
- 60093
- 49281.

Rockwell also recommends users evaluate firewall configurations to ensure other appropriate inbound and outbound traffic is blocked.

MITRE[a] has assigned number CVE-2011-3489 to this vulnerability.

----- END UPDATE 3 of 3 -----

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[b]

a. http://cve.mitre.org/cve/, website last accessed September 16, 2011.
b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, last accessed September 13, 2011.

- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods such as Virtual Private Networks (VPNs).

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

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[c]

Organizations that observe 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

ICS-CERT Operations Center
1-877-776-7585
ICS-CERT@DHS.GOV

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

c. Control Systems Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, last accessed September 16, 2011.