ICS-CERT ALERT

ICS–ALERT-11-081-01—BROADWIN WEBACCESS RPC VULNERABILITY

March 22, 2011

ALERT

SUMMARY

Independent security researcher Rubén Santamarta notified ICS-CERT of a vulnerability in BroadWin WebAccess, a web browser-based human machine interface (HMI) product. ICS-CERT forwarded the researcher's vulnerability information to BroadWin. However, BroadWin has not been able to validate the vulnerability. Today, Mr. Santamarta publicly released details of the vulnerability including exploit code.

The reported vulnerability is an RPC exploit against the WebAccess Network Service on 4592/TCP. Remote code execution is reportedly possible.

ICS-CERT is continuing to work with BroadWin to develop a solution to effectively mitigate this reported vulnerability. ICS-CERT will provide additional information as it becomes available.

MITIGATION

ICS-CERT recommends that users minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[a] 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).

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 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.*[b]

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed January 17, 2011.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

BACKGROUND

BroadWin WebAccess is a web-based HMI platform used in energy, manufacturing, and building automation applications. WebAccess is installed in several countries in Asia, North America, North Africa, and the Middle East.

ICS-CERT CONTACT

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

ICS-CERT Operations Center
1-877-776-7585

www.ics-cert.org
ICS-CERT@DHS.GOV

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.