ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-204-01—SIEMENS S7-300/S7-400 HARDCODED CREDENTIALS

July 23, 2011

ALERT

On July 23, 2011 an independent security researcher publicly announced a vulnerability affecting the Siemens S7-300 and S7-400 PLCs. The researcher claims that he was able to achieve a command shell using credentials he was able to acquire from the PLC. This claim has not yet been verified by ICS-CERT or Siemens.

ICS-CERT is currently coordinating with Siemens to validate the claim and develop mitigations. Additional information regarding the validity, impact, and mitigations will be issued as it becomes available.

Siemens S7-300 and S7-400 PLCs are used in a wide variety of industrial applications worldwide.

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

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.