ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-204-01**B**—SIEMENS S7-300 HARDCODED CREDENTIALS

UPDATE B

August 03, 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.

--------- Begin Update B Part 1 of 2 --------

On August 2, 2011, an independent researcher publicly revealed hardcoded credentials (user name and password) embedded in older versions of Siemens S7-300 PLCs.

--------- End Update B Part 1 of 2 ----------

Siemens has determined that the ability to access internal diagnostic functions does not affect the S7-400 PLCs.

Siemens has confirmed that the reported vulnerability does affect certain S7-300 PLCs. The ability to access internal diagnostic functions is present in older versions of the firmware. This includes S7-300 PLCs with integrated Profinet interface shipped before October 2009, and IM15x Profinet PLCs shipped before September 2010.

--------- Begin Update B Part 2 of 2 --------

ICS-CERT has also confirmed that the reported vulnerability affects certain S7-300 PLCs and does not affect the S7-400 PLCs.

--------- End Update B Part 2 of 2 ----------

MITIGATION

Affected CPUs and firmware versions are listed in the table below.

PLC Name	Affected Version	Fixed In	Date Fixed
CPU315(including F)-2PN/DP	V2.6 and previous	V3.1	10/2009
CPU317(including F)-2PN/DP	V2.6 and previous	V3.1	10/2009

PLC Name	Affected Version	Fixed In	Date Fixed
CPU319(including F)-3PN/DP	V2.7 and previous	V2.8	06/2009
IM151-8(including F) PN/DP CPU	V2.7	V3.2	08/2010
IM154-8 PN/DP CPU	V2.5	V3.2	08/2010
S7-400 – All Models	Not Affected		

Owners/operators utilizing these affected devices should contact Siemens Service and Support for further assistance.

Further information can be found on the Siemens Service and Support website at the following URL:

http://support.automation.siemens.com/WW/view/en/51810333

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.a

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

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.

---

a. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html