ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-129-01—SAMSUNG DATA MANAGEMENT SERVER ROOT ACCESS

May 9, 2011

ALERT

SUMMARY

ICS-CERT was made aware of a published report by an independent researcher specifying a hard-coded credential vulnerability in the Samsung Data Management Server. This vulnerability allows an attacker to remotely log in with administrative privileges via telnet or FTP. ICS-CERT has not validated this vulnerability.

MITIGATION

ICS-CERT is currently coordinating with the vendor to validate and mitigate this vulnerability. Additional information will be published as it becomes available.

The Samsung Integrated Management System Data Management Server (DMS) is primarily used to manage multiple air conditioning units in large public buildings. This product has been widely deployed in approximately 15 countries, including South Korea, various European countries, China, and the United States.

ICS-CERT encourages asset owners to minimize network exposure for all control system devices. Critical control system devices should not directly face the Internet. Local control system networks and remote devices need to be deployed behind carefully configured firewalls and isolated from the business network. When remote access is necessary, secure methods such as Virtual Private Networks (VPNs) should be used.

Security and operational organizations observing any suspected malicious cyber or control system 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 Systems Security Program (CSSP) 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.*[a]

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

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

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.