ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-069-01—SAMSUNG DATA MANAGEMENT SERVER

May 06, 2011

OVERVIEW

An earlier version of this Advisory was posted on the US-CERT Portal. This website posting was delayed to allow users time to download and install the Samsung update that mitigates this vulnerability.

Jose Antonio Guasch, an independent security researcher with Sistemas Informaticos Abiertos (SIA), reported a SQL injection vulnerability in the Samsung Data Management Server (DMS). Samsung has released an update and ICS-CERT has verified that the software update corrects the vulnerability.

AFFECTED PRODUCTS

Version 1.4.2 and all earlier versions are affected by this vulnerability.

IMPACT

The Samsung DMS is designed to automate building environment control and is used primarily by schools and other public organizations, which typically install multiple air conditioning units in their buildings.

BACKGROUND

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

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The DMS system includes an integrated web server with an application used to control multiple air conditioning systems from a centralized management console. The DMS web interface is vulnerable to a SQL injection attack, which allows an attacker to bypass authentication and access the web server as an administrative user.

VULNERABILITY DETAILS

EXPLOITABILITY

An unprotected DMS system can be remotely exploited through a SQL injection attack.

EXISTENCE OF EXPLOIT

No exploits are known that target this vulnerability.

DIFFICULTY

An attacker with low to moderate skill can exploit this vulnerability using publicly available Internet search engines to identify vulnerable systems. An attacker can bypass authentication and gain administrative privileges using uncomplicated SQL injection techniques.

MITIGATION

Samsung has released an updated version of the DMS software to address this vulnerability.

ICS-CERT and Samsung recommend that DMS users implement the following mitigation steps:

1. Download and review the update guide from the Samsung website: http://www.dvmcare.com/SRM/dms/HowToUpgradeDMSSW.pdf.
2. Upgrade DMS to the latest Version 1.4.3. To verify which version of DMS is currently running, connect to the DMS system and locate the version in the web browser title bar.

   Users can download the update at: http://www.dvmcare.com/SRM/dms/download.html.
3. Download and apply the DMS Update Plus: http://www.dvmcare.com/SRM/dms/DMSUpdaterPlus.zip
4. Implement firewall rules to limit network access to the DMS system on Port 80/TCP.

ICS-CERT encourages asset owners to minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Locate control system networks and remote devices behind firewalls and isolated from the business network. When remote access is required, use 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.*[a]

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For Control System Security Program Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

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