ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-10-301-01— MOXA DEVICE MANAGER BUFFER OVERFLOW

October 28, 2010

OVERVIEW

On October 20, 2010, an independent security researcher posted[1] information regarding a vulnerability in the MOXA Device Manager (MDM) version 2.1. MOXA has confirmed this vulnerability and is working on releasing a new version to resolve this issue.

The security researcher's analysis indicates successful exploitation of this vulnerability can lead to arbitrary code execution and control of the system. However, based on conversations with the researcher, the level of difficulty to exploit this vulnerability is high.

AFFECTED PRODUCTS

MOXA Device Manager Version 2.1 is affected by this vulnerability.

IMPACT

MOXA's embedded device products are implemented in a variety of industrial control solutions making it difficult to ascertain where and how the products are used. Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

BACKGROUND

MDM 2.1 is a freeware software product developed by MOXA for users to manage MOXA's embedded computers. MOXA devices are used in a wide variety of applications across a wide range of industries including substation monitoring, manufacturing, telecommunications, medical, etc. MOXA has offices in Taiwan (HQ), China, Germany, and Brea, California while the heaviest concentration of Moxa distributors is in the United States.

The MDM is used to remotely monitor and manage approximately 50 different embedded device products. Some functions that can be performed using the MDM software are firmware upgrades, file system management, program monitoring, process control management, network configuration, system reboots, and other management tasks.

[1] Rubén Santamarta, http://www.reversemode.com/index.php?option=com_content&task=view&id=70&Itemid=1, website last visited October 28, 2010.

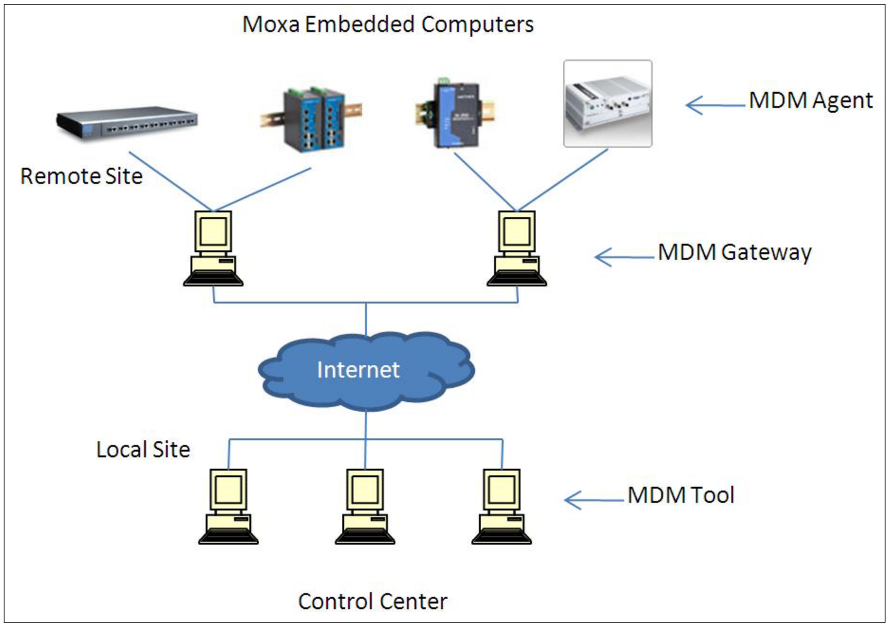
MOXA embedded computers are used for front-end computers at remote sites, for onsite data collection, and industrial control applications. Their embedded computers operate on MOXA-provided operating systems (Linux, CE, XPe).

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The MOXA Device Manager consists of an MDM Tool which allows local users to connect to a remote MDM Gateway to monitor and manage embedded computers installed with MDM Agent software.

The vulnerability is a stack-based buffer overflow caused by the use of the "strcpy" function in the MDM Tool software component.



VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability has a lower probability of being exploited.

Based on current information about the vulnerability, control of the MDM Gateway is necessary since the vulnerable function is exposed during communication between the MDM Tool and MDM Gateway. If an attacker has the capability to compromise the Gateway, exploitation of this vulnerability may not be necessary as other methods of compromise may be possible. Additionally, the MDM Tool was compiled using the /GS switch[2] and therefore forces an attacker to use additional effort[3] when constructing an exploit.

EXISTENCE OF EXPLOIT

The researcher did create an exploit during his research; however he reports that it is not 100% reliable.

MITIGATION

MOXA has stated that they are actively working to mitigate this vulnerability and will provide additional information as soon as it is available.

Based on current knowledge of the vulnerability, the following mitigations are recommended:

- Update version 2.1 to the new MDM version when it is released.
- Ensure network protection for the MDM Tool, Gateway, and Agents to protect communications between these systems.
- Encourage asset owners to minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Control system networks and remote devices should be located behind firewalls, and be separate from the business network. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be utilized.
- Refer to the Control System Security Program 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*[4]

[2] Microsoft, http://msdn microsoft.com/en-us/library/Aa290051, website last visited October 28, 2010.

[3] Litchfield, http://www ngssoftware.com/papers/defeating-w2k3-stack-protection.pdf, website last visited October 28, 2010.

[4] CSSP, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html, website last visited October 28, 2010.

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.