Important Security Notification

MiCOM C264 Product

11-Jan-2016

Overview

Schneider Electric was notified and is responding to a discovered vulnerability in the MiCOM C264 product.

Vulnerability Overview

A remotely exploitable vulnerability was identified in the VxWorks Operating System that could be exploited by attackers to gain a backdoor access to the device and/or network system

Product(s) Affected

The product affected includes:

- MiCOM C264 (Versions B4 to B10, C1 and D1.1), embedding VxWorks 5.5 to 6.9.4.1

Vulnerability Details

Due to this vulnerability, an "Integer Overflow" could be generated using RPC (Port 111). If successfully exploited, this vulnerability could lead to a remote code execution from a remote location (using the same subnet) while benefitting from the current user's privileges. Based on the VxWorks environment, confidentiality, integrity, and availability could be compromised.

CVSS Scoring

CVSS scoring is a standard way of ranking vulnerabilities and is provided for reference based on a typical control system. It is to be evaluated by individual users as required.

CVSS Base Score: 7.4 (AV:N/AC:L/Au:N/C:N/I:C/A:C)

Mitigation

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industrial best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System.

Mitigation actions are proposed to reduce risk.

- Secure the Network accesses
- Reinforce Physical Security.
- Put in place Network Intrusion Detection System (NIDS).

To Secure the Network Access, it is recommended to apply strong “hardening” rules over the Network communicating devices, such as:

- Disable unused services and ports (Secure management protocol, Physical port, VLAN)
- Least privilege
- Central Account management
- IP filtering
- MAC Change notification
- Security Logs Management

For Network Intrusion Detection mitigation, it is recommended to introduce advanced firewalls (capable of intrusion detection) in the network architecture. The Intrusion Detection System rules have to be defined according to the environmental constraints.

On-going action plan

Schneider Electric is working to develop a patch to solve the issue raised in this document.

The patch version will be delivered with the MiCOM C264 version D1.x (x > 1) and all subsequent releases.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's Cybersecurity web page at

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Strategy & Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2016.01.13 08:23:37 -05'00'