Important Security Notification

Struxureware Building Operations – Automation Server

25-Jan-2016

Overview

Schneider Electric has become aware of vulnerabilities in the Automation Server of the Struxureware Building Operations product line.

Vulnerability Overview

The vulnerabilities identified include:

- Weak credentials management
- OS Command Injection

Product(s) Affected

The product(s) or product lines affected include:

- Automation Server series (AS, AS-P), V1.7 and prior

Vulnerability Details

The system permits the user to operate the system with weak default user credentials. Users are strongly recommended to modify the default credentials to properly secure their system, but prior to version 1.7.1, it was possible to allow the system to operation with the default credentials after commissioning. The user was not forced to replace the weak default password prior to operation.

The implementation of Minimal Shell (msh) functions allow Admin users to circumvent access controls.

CVSS V2 score: 9.0 [AV:N/AC:L/Au:S/C:C/I:C/A:C]

Mitigation

Schneider Electric has released a new version of Automation Server firmware which remediates these vulnerabilities. The user is no longer allowed to operate the system with default credentials and the minimal “msh” shell can no longer be circumvented. Contact your authorized Schneider Electric service representative to execute the firmware update on the impacted devices.

Schneider Electric would like to thank Karn Ganeshen for his discovery of these vulnerabilities and his collaboration efforts to help us remediate them.

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

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2016.02.17 14:34:02 -05'00'