# ProClima Software Vulnerability Disclosure

10-Dec-2014

## Overview

Schneider Electric has become aware of vulnerabilities in the ProClima software product.

## Vulnerability Overview

The vulnerabilities identified include ActiveX controls that could be exploited to cause buffer overflow and possibly result in remote code execution.

## Product(s) Affected

The product affected:

- ProClima Software V6.0.1

## Vulnerability Details

- Atx45.ocx control can be initialized and called by a malicious script potentially causing a buffer overflow, which may allow an attacker to execute code remotely. CVE-2014-8513, CVE-2014-8514, and CVE-2014-9188 have been assigned.
  - CVSS base score of 10.0. Base vector is (AV:N/AC:L/Au:N/C:C/I:C/A:C)
- MDraw30.ocx control can be initialized and called by a malicious script potentially causing a buffer overflow, which may allow an attacker to execute code remotely. CVE-2014-8511 and CVE-2014-8512 have been assigned.
  - CVSS base score of 10.0. Base vector is (AV:N/AC:L/Au:N/C:C/I:C/A:C)

## Mitigation

Schneider Electric has released an updated version of ProClima software, V6.1.7, that mitigates these vulnerabilities. Customers are encouraged to download the new version and update their

installations. It is important that customers first uninstall the current version. The new version can be downloaded from www.schneider-electric.com. Here is a direct link to the download:

http://www.schneider-electric.com/ww/en/download/document/ProClima_software

Schneider Electric would like to thank the HP's Zero Day Initiative for their engagement and support in providing details about the vulnerability.

## 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