

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

01/28/2015

SUBJECT:

Vulnerability in Schneider Electric Software Packages Could Allow Remote Code Execution

Overview:

A vulnerability has been discovered in Schneider Electric Software Packages Unity Pro, SoMachine, SoMove, and SoMove Lite, that could allow a remote attacker to take complete control of a vulnerable system. Unity Pro is a development software to test, debug, and manage applications. SoMachine is a single software environment for developing, configuring, and commissioning automation machinery. SoMove/SoMove Lite is setup software for motor control devices.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

At this time, there is no known proof-of-concept code available.

SYSTEM AFFECTED:

- Unity Pro, all versions
- SoMachine, all versions
- SoMove, all versions
- SoMove Lite, all versions

The following Schneider Electric DTM libraries are affected:

- Modbus Communication Library, Version 2.2.6 and prior
- CANopen Communication Library, Version 1.0.2 and prior
- EtherNet/IP Communication Library, Version 1.0.0 and prior
- EM X80 Gateway DTM (MB TCP/SL)
- Advantys DTMs (OTB, STB)
- KINOS DTM
- SOLO DTM
- Xantrex DTMs

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **Medium**

Home users: N/A

TECHNICAL SUMMARY:

A DLL in a DTM development kit which is installed during DTM set up could be vulnerable to a buffer overflow that may allow an attacker to cause a buffer overflow and remotely execute code.

Successful exploitation of this vulnerability could allow the attacker to bypass certain security restrictions, gain unauthorized access, run malicious HTML and script codes, or steal cookie-based authentication credentials. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Schneider Electric has released a patch that resolves the vulnerability by removing the vulnerable DLL.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable systems running Unity Pro, SoMachine, SoMove, and SoMove Lite immediately after appropriate testing.
- Confirm that the operating system and all other applications on the system running this software are updated with the most recent patches.
- Deploy NIDS to detect and block attacks and anomalous activity such as crafted requests containing suspicious URI sequences.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Schneider Electric:

http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2015-009-01

ICS-CERT:

<https://ics-cert.us-cert.gov/advisories/ICSA-15-027-02>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>