Security Notification – Unity Simulator

14-Oct-2016

Overview

Schneider Electric has become aware of a vulnerability in the Unity PRO Software product.

Vulnerability Overview

The vulnerability is arbitrary code execution made possible by remotely downloading a patched project file to the Unity Simulator.

Product(s) Affected

The product affected:

- Unity PRO, all versions prior to V11.1

Vulnerability Details

Unity projects can be compiled as x86 instructions and loaded onto the PLC Simulator delivered with Unity PRO. These x86 instructions are subsequently executed directly by the simulator.

It is possible to make the simulator execute malicious code by redirecting the control flow of these instructions:

By implanting arbitrary shellcode in free space of a Unity PRO project, then download and execute the patched project to the simulator.

Overall CVSS Score: 7.5

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Mitigation

This vulnerability is made possible when no application program has been loaded in the simulator or when the application program loaded in the simulator is not password protected.

Mitigation of this vulnerability is realized with the following points:

- From Unity PRO V11.1 version, by default, it is not possible to launch simulator without any Unity PRO application associated

- It is up to user to select the Unity PRO default application to be launched by the simulator, and to protect this application program by a password

- Once the password protected application has been loaded onto the simulator, then it is not possible to load or to modify this application without being authenticated

Important note: It is up to user responsibility to protect his application by a proper password.

Schneider Electric would like to thank the team from Indegy, specifically Avihay Kain and Mille Gandelsman for their discovery and support during the disclosure process.

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: Schneider Electric is the global specialist in energy management and automation. With revenues of €27 billion in FY2015, our 160,000 employees serve customers in over 100 countries, helping them to manage their energy and processes in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies will reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

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: 2016.10.14 17:17:53 -04'00'