Security Notification – IGSS Software

31-Mar-2017

Overview

Schneider Electric has become aware of a vulnerability affecting the IGSS product. It relates to Windows handling of DLL's and OCX's.

Vulnerability Overview

The vulnerability identified is related to two sets of Windows files that can be hijacked. Certain OCX and DLL files are not handled securely when installed in Windows 7 environments.

Product(s) Affected

The product(s) affected:

- IGSS Software, V12 and previous versions

Vulnerability Details

In Windows 7 certain OCX files are registered with a path relative to an environment variable that seems to be resolved in a way that leads to a file search following the Windows search path. If you inject a hijacked copy of the specific OCX in the search path, then it will be executed. In Windows 10 the same OCX files are registered with an absolute path so that only that specific version is executed

In Windows 7, when looking for a specific DLL, a file search will accept and execute other versions from the same group of DLL's. In Windows 10, only the specific named DLL is searched and with an absolute path. Windows 7 installations allows a relative path to find DLL's and exposes itself to potential DLL hijacking.

Overall CVSS Score: 6.8

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

Mitigation

It is recommended that users concerned about this vulnerability to upgrade to Windows 10. Windows 10 enforces a fixed path to the DLL.

Acknowledgements

Schneider Electric would like to thank Karn Ganeshen for his reporting of this vulnerability and his efforts related to coordination of this 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

Schneider Electric is the global specialist in energy management and automation. With revenues of ~€25 billion in FY2016, our 160,000+ employees serve customers in over 100 countries, helping them to manage their energy and process 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 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: 2017.03.31 09:25:47 -04'00'