Cybersecurity Vulnerability Disclosure

Overview

Schneider Electric has become aware of two vulnerability disclosures made by Microsoft Corporation that could impact installations using Schneider Electric's software products.

Vulnerability Overview

The disclosures from Microsoft are named MS12-027 (CVE-2012-0158) and MS12-060 (CVE-2012-1856). These disclosures affect the common controls packaged in the ActiveX Control module mscomctl.ocx. Exploit of these vulnerabilities requires an external connection to a malicious web server. If successfully exploited, these vulnerabilities could allow Remote Code Execution. Microsoft classifies these vulnerabilities as Critical.

Product(s) Affected

Due to the nature of the potential risks associated with these vulnerabilities and the broad scope of the associated patches provided by Microsoft, Schneider Electric cannot provide product-specific guidance or patches targeting Schneider Electric products and strongly recommends that customers review and implement appropriate Microsoft recommendations.

Vulnerability Details

Refer to the below referenced documents from Microsoft and the National Vulnerability Database:

http://technet.microsoft.com/en-us/security/bulletin/ms12-027
http://technet.microsoft.com/en-us/security/bulletin/ms12-060
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0158
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1856

Mitigation

Microsoft has provided a patch and workaround instructions. Additionally, they have provided guidance for mitigating these vulnerabilities for systems that cannot be patched. Schneider Electric recommends its customers review and apply applicable guidance provided by Microsoft, exercising appropriate caution and leveraging offline testing to ensure that any system changes are tested thoroughly before deployment. The Common Controls affected by these vulnerabilities and the associated mitigations are used in many third party software products that may not be managed by the patch released by Microsoft.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain assistance on how to protect your installation, please contact your local Schneider Electric Customer Care Center.

For further information on disclosed 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