Security Test Report Sharing Policy

Our intent

To help protect our customers' investment in our products and solutions Schneider Electric does not provide detailed security test reports or release detailed information about specific security vulnerabilities or enhancements unless they are associated with a publicly disclosed vulnerability and resolution.

What we can do

Schneider Electric can provide a summary version of a security test report, upon request, under NDA (non-disclosure agreement), that may detail: scope, approach, qualifications, categorical results, and mitigation status, as applicable.

What our customers can do

It is essential that customers receiving Schneider Electric Security Test Report summary information *consider the content as confidential and use it in an extremely controlled and limited manner*, solely within their organization. The information, although generalized, and non-specific in details, is not for general/public distribution and consumption.

Additionally, to both maintain and improve the security posture of Schneider Electric installations, it is highly recommended that customers incorporate a defense-in-depth approach to securing their systems that covers people, technologies, processes and policies that include *patch management*. Customers should upgrade to the latest version of product software or firmware as soon as it is made available.

> **Caution:** In keeping with accepted Information Technology (IT) and Operational Technology (OT) best practices, all patches should be installed and tested for compatibility with system components in a non-production/test environment prior to roll-out, to avoid unintended impacts to their live systems.