UL2900 and Trellix / Wavelinx system

What is UL2900?

UL2900 is a series of standards published by UL (formerly Underwriters Laboratories), a global safety consulting and certification company. The standards present general software cyber security requirements for network-connectable products (UL2900-1), as well as requirements specifically for medical and healthcare systems (UL2900-2-1), industrial control systems (UL2900-2-2), and security and life safety signaling systems (UL2900-2-3). It is worth noting that the American National Standards Institute (ANSI) has adopted UL2900-1 as a national consensus Standard and that the FDA has also officially recognized the UL2900 standard for connected equipment being installed in healthcare facilities.

Why is UL2900 important?

As products are becoming more and more interconnected, the cyberthreats used by attackers to manipulate software vulnerabilities and weak links in ecosystems grows exponentially. UL2900 is important because each device connected to the internet is a potential attack point for cyber criminals. Attacks are becoming more sophisticated, more difficult to protect against, and costlier than ever.

According to Gartner, there will be 5.8 billion enterprise and automotive Internet of Things (IoT) endpoints in 2020, a 21% increase from 2019. According to a 2018 report from Trustwave, "Sixty-one percent of [organizations] surveyed who have deployed some level of IoT [Internet of Things] technology have had to deal with a security incident related to IoT."

According to federal agencies in the United States, there were 31,000 cyber security incidents reported in 2018. While a study undertaken by IBM Security and Ponemon estimated that the average cost of data breach was $3.9M in 2019.

To achieve wide adoption of IoT technologies within the commercial space as well as unlock the vast potential of the IoT systems, manufacturers must build cybersecurity into their connected products to not only protect consumers and businesses but themselves.

What do the UL2900 standards cover?

Scope of UL2900-1

Cooper Lighting Solutions has obtained UL2900-1 certification for its network-connectable products such as Trellix Core Pro and WaveLinx Wireless Area Controller.

UL2900-1, the UL Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, was published and adopted as an ANSI (American National Standards Institute) standard in July 2017.

The UL2900-1 standard says it "applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware" and that it describes these requirements and methods:

1. Requirements regarding the software developer (vendor or other supply chain member) risk management process for their product.
2. Methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses, and malware.
3. Requirements regarding the presence of security risk controls in the architecture and design of a product.

Types of security assessment included in UL2900-1

The UL2900-1 comprehensive testing addresses all aspects of the product from documentation, hardware and software assessment. The UL2900-1 cybersecurity assessment can be divided into three main sections:

1. **Document for Product, Processes and Use**
   UL assesses the product documentation ensuring that the document provides the required information to users to secure their system and overall process used to manufacture and distribute the product.
2. **Risk Controls and Management**
   UL reviews how the product manages access control, user authentication and authorization. It will also assess how users can access the device remotely, i.e. they would assess all the interfaces available on the product (ethernet, HDMI, USB, etc...pability, i.e. mechanism used to encrypt and decrypt data that enables the product to store sensitive information or transmit it across insecure networks so that it can be read only by the intended recipient or application.
3. **Product Assessment**
   UL evaluates the product for known malware, vulnerabilities reported under the NIST National Vulnerability Database (NVD), common software weaknesses in source code, and malformed data on various protocols and interfaces that would be accessible to an outside party. It also assesses vendor's risk assessment plan and performs a structured penetration testing including attempt to engage product in a denial of service, attempt to access by unauthorized means, attempt to exploit vulnerabilities and attempt to circumvent risk and security controls. Finally, they would also conduct a series of test such as Static Application Security Test (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST) and Software Composition Analysis (SCA).

Why did we choose UL?

We believe that if done well, a certified product from a reputable organization such as UL2900 will mitigate risk associated by cyber threats, protect our brand reputation and establish market leadership by creating product differentiation.

The Gartner report forecasts that the building automation market, driven by connected lighting devices, such as Cooper's WaveLinx connected lighting system, will be the segment with the largest growth rate in 2020 (42%) within the IoT space, followed by automotive and healthcare, which are forecast to grow 31% and 29% in 2020, respectively.

To provide the safest connected lighting system in the market, we needed a third-party company to test our products in addition to our in-house cyber security team.

While other cybersecurity certifications are available, the UL2900-1 compliance standard is specific to network-connectable products and UL, as a testing company, is globally recognized with experience promoting safe environments since 1894. The range of products that can be addressed with UL2900-1 includes the range of systems that are offered by Cooper Lighting Solutions including our WaveLinx Area Controller and Trellix Core Pro. Under the Cooper Lighting Solutions' Cyber Protection Product Security Program, we are focused on enhancing the cybersecurity of our products, so partnering with an industry known company to certify our practices is another way we can bring peace of mind to our customers.

What are the benefits of UL2900 certification?

As UL notes, "By incorporating an IoT platform that is already UL certified with your products, you can … [streamline] your product's UL certification with less cost and faster time to market. By maximizing your security rigor with vendors that are already UL certified, you are minimizing supply chain risk and increasing trust in your brand."

UL also lists these benefits of UL CAP:

Risk mitigation. Cyberattacks can expose your customers to unscrupulous hackers. Take proactive steps to protect your brand from security risks.

Innovation. Incorporate IoT security into quality assurance programs and establish baseline security standards for partners and suppliers to follow.

References

1. UL IoT Security Top 20 Design Principles,
   https://ims.ul.com/sites/g/files/qbfpbp196/files/2018-05/iot-security-top-20-design-principles.pdf
2. Gartner News Room, "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020",
   https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io
3. UL cybersecurity Assurance and Compliance web site:
   https://www.ul.com/offerings/cybersecurity-assurance-and-compliance

COOPER Lighting Solutions

Cooper Lighting Solutions
1121 Highway 74 South
Peachtree City, GA 30269
P: 770-486-4800
www.cooperlighting.com
For service or technical assistance:
1-800-553-3879

Canada Sales
5925 McLaughlin Road
Mississauga, Ontario L5R 1B8
P: 905-501-3000
F: 905-501-3172