Counterfeit product primer

Counterfeit products: Background

Nearly all companies producing profitable, high-demand products face the threat of having these products counterfeited. The emergence of counterfeit networking hardware is not a new phenomenon; examples of counterfeiting were first observed by Cisco in the early 2000s. Counterfeiting can be broadly described as applying a company's logo without its permission. In the case of Cisco® products, it generally involves applying the bridge logo shown in the upper right hand corner of this page and product model numbers without Cisco's authorization.

Counterfeit products: Analysis

Counterfeit Cisco products pose many dangers, the most common of which are described below.

The design and performance of a Cisco product is directly related to the quality of its components, necessitating Cisco's careful evaluation and selection of the components specified for each product. Counterfeiters often use different components than those found on genuine Cisco products. This is done to reduce the cost of the end product created by counterfeiters. Component substitution places the product safety certifications (i.e., CSA, TUV Rheinland, UL, etc.) at risk and can affect the performance of the product. Processors and fuses, in particular, are commonly substituted components found on recovered counterfeit Cisco products, and both play a sizable role in determining product performance and safety compliance.

Search warrants conducted by law enforcement agencies reveal that counterfeiting operations are extremely rudimentary, with many components intended for sophisticated surface-mount soldering processes instead installed by hand with a simple soldering iron. Work areas inside counterfeiting operations are heavily cluttered, and very little to no Electrostatic Discharge (ESD) controls are present to prevent latent or early component failure(s). In contrast, Cisco production facilities are tightly regulated, and personnel movement, materials, and electronic component soldering processes are closely tracked and automated wherever possible. Cisco factories also employ numerous methods to minimize ESD events throughout the build and test processes.

Power supply substitutions have also been observed on counterfeit Cisco products. In some Cisco products, power supplies can be installed and/or replaced by the user. In others, the power supplies are internal to the unit and are not designed to be replaced by the user. In both scenarios, counterfeit products have been found in which the included power supplies differ from the genuine Cisco configurations. Altered power supplies can pose a multitude of risks to both the user and the equipment, as they plug directly into a 110- or 220-volt source (depending on location).

Product testing is another function observed to be notably lacking at counterfeiting locations. Genuine Cisco products undergo a great deal of testing during both the design phase and the manufacturing phase. The testing is designed to stress the units under a variety of harsh conditions, and product defects are fed back into the design to drive improvements. Counterfeit Cisco products, however, do not exhibit this level of detailed testing. Evidence recovered at counterfeiting operations indicates that only the most basic functionality testing is performed.

On the software side, Cisco sells licenses to use its copyrighted software with most hardware products. Cisco does not allow third parties to resell licenses, which means that at a minimum, counterfeiters are using pirated versions of Cisco software. There also remains the potential that counterfeiters may produce compromised boxes with back doors or malware installed. There is simply no guarantee that counterfeit products will operate identically to genuine Cisco devices.

Conclusion

Counterfeit products present potentially serious risks to network quality, performance, safety, and reliability. Careful study of counterfeit Cisco products reveals that:

- Substitute electronic components (processors, fuses, etc.) used in counterfeit products often do not meet the performance standards found in genuine Cisco products and have not been subjected to the same degree of system-level quality and performance testing.
- Counterfeit products do not hold the same safety standard certifications that genuine Cisco products attain. Changes to power supplies have also been observed, which not only pose risks to safety certifications but can also put the equipment and its operator at risk.
- Very little to no electrostatic discharge equipment is employed in the manufacture of counterfeit Cisco units, increasing the risk of equipment failure.
- Counterfeit products are running pirated copies of Cisco software and therefore do not carry valid software licenses. Further, there is no guarantee that software running on counterfeit products will operate in the same manner as genuine Cisco software.

Contact the Cisco Brand Protection team at brandprotection@cisco.com should you have any questions about the authenticity of your Cisco products.

C02-740750-00 07/18