filename:comptia-secplussy0601-1-14-vulnerabilities
Showname: Security+ \(SY0-601\)
Topic: Threats, Attacks and Vulnerabilities
Episode: Vulnerabilties
Learner Objectives:

Explain the security concerns associated with various types of vulnerabilities.

Description: In this episode, the viewer will identify situations that lead IT infrastructure into vulnerable positions such as weak configurations, third-party risk, weak patch management and legacy platforms.

---

* Weak configurations
    + Open permissions
    + Unsecure root accounts
    + Weak encryption
    + Unsecure protocols
    + Default settings
    + Open ports and services
* Third-party risks
    + Increase risk for
        - Intellectual Property Theft
        - Identity/credential theft
        - Network Intrusion
        - Reputation damage \(Think Target\)
        - Lack of vendor support
        - Data storage/Data Breach/Data Theft
        - Cloud-based risk
    + Vendor management
        - Problems
            * Compliance risk
            * Vendor Reputation
            * Lack of Visibility
        - Benefits
            * Screening
            * Risk Management
            * Compliance
    + System integration
        - Social Networks \([Facebook])

        - Delivery Systems \(USPS,UPS,FedEx\)
        - Online payment systems \(Paypal)
        - Video streaming services \(YT, Vimeo\)
    + Outsourced code development
* Improper or weak patch management
    + Firmware
        - Current Firmware 2.0.2.188405
        - [CVE-2019-7579]
    + Operating system (OS)
    + Applications
* Legacy platforms
* Zero-day

[Facebook]:https://developers.facebook.com/docs/facebook-login/multiple-providers/

[CVE-2019-7579]:https://www.cvedetails.com/vulnerability-list/vendor_id-833/Linksys.html