

Network Protection for Design Professionals

Security Patches

Background:

Security patch management — updates or patches are regularly provided by software vendors to fix problems within their products. Many of these patches fix vulnerabilities, which could be exploited by attackers.

How to implement appropriate controls:

Subscribe to patch notification services from vendors for software utilized, review and evaluate at least weekly, preferably daily. Where possible, enable automatic update capabilities. Test and install critical security patches and upgrades within 24 hours of availability and no later than 30 days for all patches.

Formal patch management procedures should include the following:

- An inventory of IT resources, hardware equipment, operating systems, and software applications used within your organization.
- Monitoring of security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within your system inventory.
- Priority system for the order in which your organization addresses remediating vulnerabilities.
- Testing of patches and non-patch remediations on IT devices that use standardized configurations. Make sure the remediation will not disrupt operations or degrade security elsewhere on your network before implementing in your production environment.
- Automated deployment of patches to IT devices using enterprise patch management tools.
- Automatic update of applications whenever possible and appropriate.
- Verification of vulnerability remediation through network and host vulnerability scanning.

Further information on patch and vulnerability management procedures can be found in:

The National Institute of Standards and Technology's Creating a Patch and Vulnerability Management Program,

<http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

