

1. Overview

Computers are typically attacked within seconds of being connected to the U of A network – systems which are not “patched” to protect against these attacks will be compromised immediately. This is very common with brand new or reinstalled systems, which are often connected to the network “just to patch software”, and are compromised during this process.

All software requires regular maintenance to remain secure; this maintenance comes in the form of patches or updates. As new ways to exploit weaknesses are discovered, software vendors release patches to correct problems in the software. Patches can usually be downloaded from the vendor’s homepage, while some vendors provide a means to automatically download and install them. It is important that patches be installed as soon as possible after they are released; attackers often develop exploits shortly after the vulnerabilities are discovered.

2. Purpose

The following guidelines will assist university affiliates in updating and securing networked computers. Departments and individuals are encouraged to contact local computer support for assistance in implementing these procedures. These guidelines should not be used to diminish existing procedures.

3. Scope

These guidelines apply to all computers connected to the university network. This includes computers situated behind firewalls or using a VPN.

4. Guidelines

Microsoft Windows patch updates

1. Automatic Updates
2. Windows Update: <http://windowsupdate.microsoft.com>
3. Office Updates: <http://office.microsoft.com/en-us/officeupdate/default.aspx>
4. Subscribe to Microsoft Security Notification Service

Apple Macintosh patch updates

1. Automatic Updates
2. Subscribe to Apple Security Notification Service

Linux OS patch updates

1. Subscribe to mailing list for your distribution

Unix OS patch updates

1. Check vendor's website for available options
2. Subscribe to applicable mailing list(s)

Application Software patches

1. Visit vendor's website regularly to check for updates
2. Register to receive email notification of updates

5. Related Guidance

Information Security Terms Guideline (IS-G100)

Standards, Procedures and Guidelines at <http://security.arizona.edu>

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

Revision History

| | |
|----------------|---------|
| Initial Draft | 5/25/06 |
| Effective Date | 5/27/08 |