



SOFTWARE SECURITY PATCHES

QUESTIONS?

If you have questions about patches, hot-fixes, or upgrades, please contact:

- Your Network Administrator / Information Technology Support Staff
- The Department of Information Systems' Customer Care Center
(501) 682-HELP (682-4357)
DIS.CallCenter@mail.state.ar.us
www.dis.state.ar.us/care_ctr

Suggested email lists to join for security vulnerability information:

<http://www.sans.org>
<http://www.cert.org>

State of Arkansas

Office of the Executive
Chief Information Officer



State Security Office

SOFTWARE SECURITY PATCHES

Aggressive security patch management is an important part of an effective information technology security strategy. Unpatched vulnerabilities leave systems open to compromise and result in unavailable information technology resources for extended periods of time.

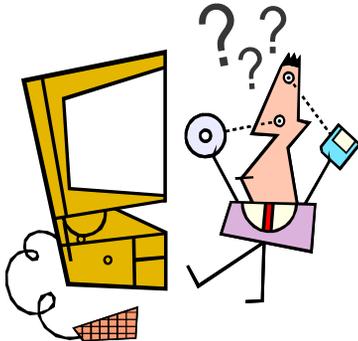
Software vendors issue patches when vulnerabilities are identified.

Security patch review and installation for operating systems, applications, and other types of software will help provide protection from security breaches.

BE AWARE THAT . . .

A patch may interfere with other applications and/or the operating system(s) on your machine.

A patch may also be faulty and may cause unpredictable results. Testing the impact of patches is critical.



SOFTWARE SECURITY RECOMMENDATIONS

- All software security patches that are labeled as critical should be reviewed and applied within a few days of their release.
- All machines with confidential or critical data or functions should be considered for all levels of patches regardless of the patches criticality.
- All patches not labeled as critical should be reviewed and applied when feasible to machines without confidential or critical data or functions.
- When possible, make a backup of a machine before applying a patch.
- All patch levels for machines in organizations should be reviewed periodically.
- Roles and responsibilities of staff in patch review and application should be defined.
- A patch might interfere with other applications and the operating system(s) on your machine.
- Research should be done to assess the impact of patching because some patches can pose problems when applied.
- Having a test environment for patches is desirable.
- Check for restoration of default settings after applying a patch. Default settings create vulnerabilities themselves.