

## **Patch Management Assessment**

A Configuration Management Plan by definition already considers change management, risk management, and patch management. Patch management should be implemented according to those larger policies. Even as risk management directly affects security, so does patch management. For this reason, it is necessary for FSA to specify standards for patch management.

### **Best Practice Requirements for Patch Management**

#### **Take an inventory of entire IT infrastructure.**

Inventory should tell you:

- The systems that make up the FSA environment
- Operating systems and application, including version
- What patches have been applied.
- Ownership and contact information.
- Any known vulnerabilities to your systems and threats that could exploit them

#### **Do quarterly updates of the inventory.**

#### **Be aware of new patches**

- Be aware of what patches are available and what the patch is meant to do (what is it fixing?). Identify and use only trusted sources for patches.

#### **Discuss applicability of patches**

- Discuss with those familiar with the system to find out if the patch is applicable. Blanket recommendations issued by vendors and organizations such as CERT and SANS tend to be broad, and err on the side of safety and caution. (For example a recommendation was given to apply a Microsoft patch pertaining to SNMP vulnerabilities. However, if the patch bulletin was read carefully it showed that it was only necessary to patch machines where SNMP was actually running, as many times it is turned off). You may want to still patch the machines but the priority and urgency to do so is much lower.

#### **Is there a better way than using a patch?**

- Review system and network processes. Even if the patch is applicable there may be better ways to deal with it. In the case of SNMP vulnerability some people just blocked SNMP traffic coming into the network firewall. This saved time and the expense of applying a patch to hundreds of desktops.

#### **Test bed the patches first**

- Test patches before applying them to production systems, as software patches frequently create compatibility issues and even vulnerabilities in other areas.

**Total Security? Be Cautious**

Remember to be cautious – Vendors are often quick to provide a solution and quick solutions that do not usually include the impact to overall security. When testing the patch be aware of how it affects overall security – does it create another type of security hole?

**Sharing Alerts, Notices and Patches**

A standard notification process should be established so all FSA systems can be made aware of vulnerabilities and their patches as quickly as possible. This may also include a path/time-frame of requirements from EDCIRC.

**Large networks need Patch Management tools**

Without patch management tools network administrators essentially track patch status in their heads, fixing holes on the fly. However, the sheer complexity of networks and number of patches makes this approach ineffective. Fortunately, there are patch management tools available.

From <http://www.nwfusion.com/supp/security2/patch.html>

Practical patch management

By Steve Ulfelder

Network World, 10/21/02

**Patch Management tools**

Patch-management tools are available from a variety of vendors, including these market leaders:

Vendor	Product	Pricing	Description
BigFix	BigFix Enterprise Suite	\$30 per seat	Delivers patch information to all computers on a network; includes management tools and an application that monitors patches and vulnerabilities in each client and server.
Configuresoft	Enterprise Configuration Manager (ECM) and Security Update Manager (SUM)	ECM starts at \$995 per server and \$30 per workstation; SUM at \$25 per server and \$5 per workstation.	ECM change-management software gathers information from clients and servers and centralizes it in an SQL2000 database; SUM, an ECM adjunct, uses Microsoft's XML Security Database and ECM data to conduct vulnerability assessments and download patches.
PatchLink	PatchLink Update	Starts at \$1,250.	Detects patch-related security holes across operating systems. It lets administrators customize patch rollouts by setting such parameters as Force Reboot and Uninstall/Roll back.
Shavlik	HFNetChkLT;	HFNetChkLT is free;	HFNetChkLT and HFNetChkPro

Technologies	HFNetChkPro; EnterpriseInspector	HFNetChkPro starts at \$900; EnterpriseInspector costs \$7,900 for up to 250 computers (HFNetChkPro customers get 50% off).	command-line utilities let network managers check to see if server configurations are up to date and have all needed security patches; EnterpriseInspector evaluates patch installations and security vulnerabilities in Windows systems.
Source: Network World			

**There is no perfect solution**

There is not a perfect solution to security and there is not one for patch management either. However, very good solution and procedure sets can be created.

**Current Patch Management Policy and Documentation at FSA**

Patch management can only rightly be seen as one component of security management in general. More specifically, patch management is a subset of Configuration and Change Management. Patch management is also closely linked to Incident Response as the confidentiality, integrity and availability of FSA systems depends in a large part on the preventative security measures taken to deter or inhibit attacks.

Section 3.7 of FSA’s Information Technology Security and Privacy Policy (FSA Security Policy) is specifically written to address Configuration/change management. Further, a recent review of FSA system security documents has shown that all FSA systems have written a Configuration Management document that adheres to the Configuration Management guide provided through the Department.

Section 3.8 of the FSA Security Policy, on Incident Response, also underlines the need for preventative Security.

**Current Patch Management Implementation**

FSA is committed to implementing the full configuration management process, including patch management, not just a subsection of it. FSA relies almost exclusively on contractors to run and maintain its systems. These contractors are made aware of all requirements as they are developed. With the current contracts stipulating Service Level Agreements (SLAs), contractors typically have some form of robust patch management or configuration management already implemented even if it is not specifically mentioned in the contract.

Furthermore, FSA has started a project to ensure that patch management is being directly addressed, and to provide guidelines for it. At the completion of the project FSA will require the contractors to fully implement the FSA configuration management and patch management policies. To do so will likely require contract modifications.