

Summary of Patch Management Research Best Practices, Current FSA Practices and Comments

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.

1.0 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
- Their operating systems and application, including version
- What patches have been applied.
- Ownership and contact information.
- Any known but un-patched threats to your systems and vulnerabilities in 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 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 the 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

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.

2.0 Current Patch Management Policy, Documentation and Implementation at FSA

The following is taken directly from the FSA Security Incident Implementation Guide and describes the process now used by FSA to handle patch management issues.

2.0 INCIDENT PREVENTION

“An ounce of prevention is worth a pound of cure” is an old saying. This saying is particularly true for IT infrastructure. Practical experience has proven that the large majority of computer incidents can be avoided by taking small, appropriate and timely measures. All FSA systems are required to prevent incidents by deploying proven software and devices including Anti-virus products, Intrusion Detection systems and devices, firewalls, and Patch Management tools and techniques. However, all these preventative measures and devices will only be effective if 1) the system uses them appropriately based on its design and security needs and 2) by keeping all the software and devices updated, patched and configured properly.

The use of Patch Management techniques and tools are therefore essential to an effective incident response program. Properly deployed, patched and updated software/hardware is difficult to compromise but improperly or un-patched/un-updated items are the reason for most of the incidents that occur. This section will cover patch and update management information at FSA

2.1 Patch and Update Management

Patch management is only one component of effective security management. The confidentiality, integrity and availability of FSA systems also depends on the preventative security measures taken to deter or inhibit attacks. More specifically, patch management is a subset of the Configuration and Change Management processes. As mentioned above, Patch management is also linked to Incident Response

Section 3.7 of FSA's Information Technology Security and Privacy Policy (FSA Security Policy) is specifically written to address Configuration/Change management. Furthermore, all FSA systems are required to have written Configuration Management document that adhere to the Configuration Management guide provided by the Department.

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

FSA is required to report to the Department on their systems with regards to specific patches and/or updates. The Department, in turn is required to report to FEDCIRC. The ability to rapidly report on system compliance is already required. This suggests that automated patch management tools, which can easily supply such information for large networks, are expected to be in place.

To help systems personnel meet the federal requirements, as they exist now, FSA has established an email alert process that informs system personnel of new security fixes, patches and problems. It has also established a process for tracking and reporting compliance with the implementation of patches and fixes.

2.2 Procedures for IT Security Alerts

The FSA Security and Privacy Team (S&PT) issues two categories of IT security alerts -- low-to-medium-level alerts and high-level alerts, which are also identified as Critical Alerts. Each category requires action by an FSA contractor and/or the system's System Security Officer (SSO). Although the low-to-medium alerts are of interest and need appropriate action taken, they can usually be scheduled so they don't interfere with normal business operations. On the other hand, high-level or critical alerts need immediate action taken to prevent an imminent security incident that could deny access, release private citizens' data, damage the Department's reputation, or incur major expenses for reconstitution of the system.

2.2.1 Low-to-Medium Alerts

The FSA S&PT regularly forwards IT security alerts to the System Security Officers (SSOs) for their systems. These alerts are routinely disseminated on Tuesdays and Fridays. Normally, these alerts contain a mixture of low- and medium-level vulnerabilities. When the routine Tuesday and Friday alerts are issued, SSOs are expected to pass the information on to the technical support staff for their systems, be it a government employee or contractor employee. Together with such staff, the SSO will determine which of the alerts contain vulnerabilities that pose a risk to their system, and take appropriate action to prevent the threat or attack from affecting the system. There is currently no requirement to report on the status of the threat/vulnerability/remediation effort for any of the low-to-medium-level alerts, though the SSO should be ready to respond to any inquiries concerning these alerts.

2.2.2 High-Level or Critical Alerts

When a high-level or critical alert is issued by FedCIRC, OMB, a manufacturer, or another source, the FSA S&PT will *immediately* issue the alert to both the appropriate SSOs and contractor contacts. For systems residing at the Virtual Data Center (VDC), CSC staff will be notified along with the VDC SSO. The SSO and contractor contacts for systems with components external to the VDC will also be notified. A list of contacts for the alerts is maintained by the FSA CSO. SSOs should check with the CSO to update the contact information for their systems. Periodically, the list will be disseminated for updating, but changes to the contact list should be forwarded to the S&PT as soon as they are applicable.

- High-level or critical alerts will be issued by first by email and then by telephone when an email acknowledgement has not been provided or for follow up. When an alert requires immediate action, the email message will bear a specific title such as those in the examples below:
 - **Special Threat Alert & Response (STAR) – Immediate Action Required**
 - The opening paragraph of the alert will provide a description of the special action needed as well as a reminder of the contact information for people on the S&PT. Technical details of the alert will also be included in the email message either as text or as a file attachment.
- When a “**STAR**” alert is issued, the “owners” of the IT systems to which the alert is directed are responsible for reporting the status of remediation efforts. This reporting can be done by either the SSO or the contractor contact. In either case, the other party must be included as a cc: for the message.

- An FSA reporting form identifying the number of affected components, the number of fixes, and the dates those components were patched along with other pertinent information will be included with each new STAR alert. If there are special reporting formats required by OMB, ED CIO, or other government agency with oversight responsibility they will also be provided with the alert.
- A report must be filed within two hours of receipt of the alert. Send the report to the S&PT member who sent the alert. The initial report can be a simple acknowledgement that the alert was received. Remediation decisions, installation of system patches or work-arounds, and other pertinent status information will be conveyed in timely follow-up reports. Upon occasion, government agencies or offices with oversight responsibility may request reports within a shorter time period.
- In any case, reporting and remediation of critical vulnerabilities will be given high priority by the system owner and system manager, and any decision to delay actual remediation (by using work-arounds) must be agreed to by the system manager. If sound business reasons exist to delay applying a patch or installing an upgrade that could/would remediate the threat/vulnerability, the system manager must state in writing the reason for the delay and must obtain concurrence of the FSA CIO.
- When a work-around is used in place of full remediation, the status for that system will be kept “open” until remediation is accomplished. Both on-going remediations as well as a final report should be filed once full remediation is accomplished.

2.3 Tracking

FSA S&PT will maintain a data system that allows the status of each critical vulnerability to be tracked for each system.

Current Patch Management Implementation

It needs to be recognized that FSA relies almost exclusively on contractors to run and maintain their systems. The contractors are made aware of all requirements as they are developed. With the current contracts stipulating Service Level Agreements (SLAs) *it is assumed that contractors typically have some form of patch management or configuration management already implemented even if it is not specifically mentioned in the contract.*

3.0 Patch Management Issues at FSA

Patch management is a necessity.

An automated tool is recommended to accurately assess patching needs, to be made aware of patches, to distribute patches and to more easily assess patch coverage.

At FSA there is no centralized IT management for all systems, rather it is the individual contractors that must patch the systems they are responsible for. The contractors may use manual methods or use a patch management tool as long as it systems are covered and information on coverage can be gathered when requested.

A patch management tool usually work with agents that are placed on all machines. FSA will need to identify how to employ a tool for GSS' and MAs so that control for patching is given to the proper group.

It is relatively easy to find patches and fixes for GSS' and for MAs if they are COTS products. If they are home grown apps then the patches come from within. How is that managed?

FSA must decide whether or not it wants to require the use of a specific patch management tool and then to purchase multiple copies of the tool for each of the different contractor sites. Or FSA could simply and overtly require patch management providing some minimum standards and requirements and to let the contractors decide how it will be done.

FEDCIRC patches and alerts VS Commercial Services

FEDCIRC is free, right now. But you are dependent upon them. FSA and the Dept. have previously had great success by their independent approach and have several times fixed areas that the FEDCIRC was slightly behind on. Relying on commercial products/services for patch management is likely to be more reliable and responsive. FSA must consider how the Patch program with FEDCIRC will work - can a contractor receive the patches directly form FEDCIRC or must it go through the government agency first. If that is the case it slows the process down.

A full time position?

Patch management can easily be a full time position and probably should be, and whether it is done via the FEDCIRC or commercial products there will be a cost.