

Enterprise Security Patch Management Policy (Draft) Federal Student Aid (FSA) Systems and Data Centers

Purpose

The purpose of this policy is to ensure that timely and continuous security patch management is practiced to:

- (1) Remediate known software vulnerabilities and thereby minimize threat exposure; and
- (2) Comply with the Federal, Department of Education, and FSA security policies, guidelines and procedures.

It is also the purpose of this policy to enable the organization to fulfill these objectives by providing the resources necessary. Resources are the people, time, and money required to perform vulnerability assessment, patch acquisition and testing; maintenance to put patches into production; updating configuration and change management documentation; and ensuring compliance through accountability.

Background

FSA has ___ systems comprised of approximately _____ servers running various operating systems, databases, middleware, and other enterprise software technologies. The operating systems for primary business systems and databases are predominately Unix though there are a substantive number of auxiliary systems running on Windows NT/2000.

Most of FSA system's production environment resides in the Virtual Data Center (VDC) located in Meriden, Connecticut. The VDC is administered by a contractor and managed by FSA personnel. The VDC contractor is responsible for all hardware, connectivity, network and machine operating systems, configuration, security, and maintenance guided by service level agreements. The data center contractor also performs maintenance on applications in coordination with the system contractor. The applications running on system servers are the responsibility of the system owners and are generally administered by contractors.

FSA's Security Incident Implementation Guide section 2 – "Incident Prevention" is superseded by this policy.

Scope

Security patch management is the practice by system or network administrators of acquiring, testing, and applying patches to remediate known vulnerabilities in information systems software.

Enterprise Security Patch Management (ESPM) is FSA's organization-wide program to enable compliance with this policy.

Enterprise Security Patch Management Policy (Draft) Federal Student Aid (FSA) Systems and Data Centers

ESPM Provides

1. Means to know system and enterprise-wide, real-time inventory of assets including:
 - a. Hardware
 - b. Operating Systems and applications including version
 - c. What patches have been applied
 - d. Logs
 - e. Associated ownership and contact information
2. A real time database of known vulnerabilities including recommended procedures for remediation from only the top reliable sources.
3. Tailored, system specific policy, guidelines, and procedures for testing, change and configuration management.
4. A means of cross-referencing asset information with known software vulnerabilities and procedural guidance/compliance to calculate the remediation requirements.
5. A centralized database of patches, their dependencies, and
6. Automated reporting and workflow

This policy applies to all systems including system servers, their network environment, and auxiliary devices that support FSA information assets. It is also meant to provide guidance on relationships with Non-FSA interconnected systems subject to security patch issues that cannot be governed by this policy.

Policy

Ownership and Responsibilities

FSA security guidelines require system managers to “Maintain a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat source, including those accepted as risk-based decisions.”¹

Computer Security Officer (CSO)

¹ Security Roles and Responsibilities June, 2003

Enterprise Security Patch Management Policy (Draft) Federal Student Aid (FSA) Systems and Data Centers

- Certify that security patch management practices comply with government-wide and department policies, regulations, and standards.
- Ensure that the system manager understands his/her responsibilities for security patch management.
- Manage and Monitor compliance with system specific security patch management directives

System Owner (SO)

System Manager (SM)

System Security Officer (SSO)

Each FSA system and data center or NOC, is assigned a System Security Officer (SSO) who is charged with applying best practices to improve the security posture of their respective system/data center. An important component of the SSO's responsibilities is the ongoing process of "identifying system vulnerabilities and risks able to recommend solutions to mitigate those risks."²

System Administrator (SA)

Users

Action

Any Action Guidelines

Monitoring and Compliance

Enforcement

Definitions

Revision History

Approval and Issuing Authority

² FSA System Security Process Guide V.4.0 February 2004