



NASA Standard Operating Procedure

Patch Selection and Reporting Procedures

Document Number: ITS-SOP-0012

Version: Revision-2

Effective Date: July 2007

Expiration Date: December 2010

Responsible Office: Office of the Chief Information Officer

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Basic	1	12/01/05	Rev 1 of the Agency patch selection and reporting procedures
Rev Draft	2	05/31/07	Updated to add Agency ERS reporting requirements
Rev Draft	2	07/11/07	Updated with Center comments
Basic	2		Signature

Patch Selection and Reporting Procedures

1. Introduction

An effective patch management program is one of the best defenses against network attacks. The following procedure provides the guidelines and schedules for reporting on systems with a PatchLink agent installed, as well as, waived systems. It also provides the patch selection criteria that will be used to form the Patch Management Baseline (PMB).

Although this procedure does not require reporting for all systems, NASA's NPR 2810 does require patching for all systems. Once reporting procedures are worked out for non-waived systems, all waived systems will be included in the reporting requirement. Before additional reporting requirements are presented to the Centers, an updated draft SOP will be circulated to ensure Center feedback is captured and addressed.

2. Scope

This document describes the patch status reporting schedule, the patch selection criteria for the Patch Management Baseline (PMB), and the reporting process, including the Enterprise Reporting System (ERS). It is applicable to all Centers within the Agency.

3. Definitions

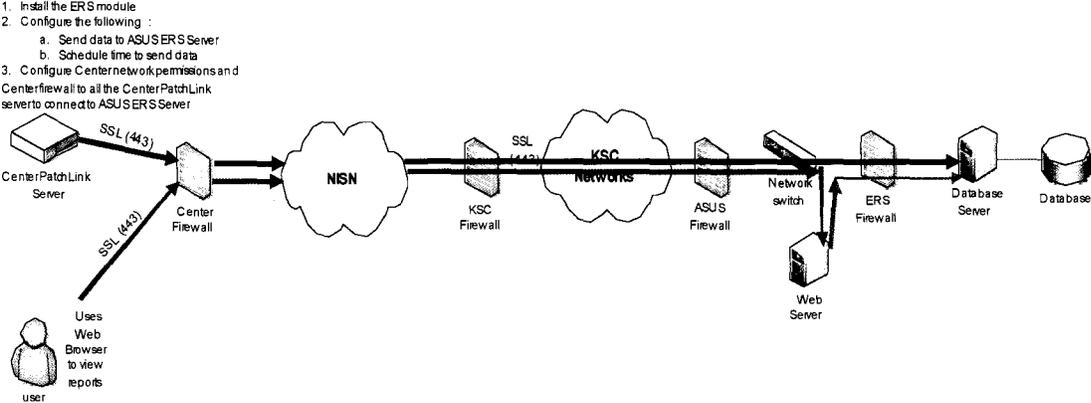
Agency Security Update System (ASUS) Project - The ASUS project is a part of the NASA Information Technology Security Program, which is under the management of the NASA CIO. This project provides NASA organizations with tools, processes, and procedures that facilitate patch management and reporting.

Networked System - A networked system has a physical or logical connection to a NASA administrative/institutional/mission network and/or a physical or logical connection to the Internet. This includes systems that infrequently connect to the Internet in the course of normal use, such as laptops.

Non-Networked System - A system not connected to any NASA administrative/institutional network. This system shall be on a stand-alone network with no physical (air gapped) or logical connection to a network based security threat vector (example: a network that has access to the Internet). Infrequent or sporadic connections to internal networks and/or the Internet are not permissible.

Enterprise Reporting System (ERS) - An Agency central database utilized to collect patch vulnerability, software inventory, and hardware inventory from each Agency PatchLink server.

The following high level diagram shows a Center PatchLink server network path to send an encrypted database snapshot to the Agency ERS Database server. In addition the diagram shows a user connecting to the ERS web server to view a report thru a web browser. The web server pulls the data from the Agency ERS database and displays back to the user.



Patch Management Baseline (PMB) - a list of critical patches to be deployed and reported upon.

PatchLink Enabled System - A computer system with an available PatchLink software agent installed and is operational.

System - A single networked host or grouping of hosts under a common technical network, or administrative boundary. Examples include computing resources such as desktop computers, rack mounted servers, and laptop computers.

Unsupported System - A computer system for which a PatchLink agent does not exist.

Waivered System - A non-PatchLink enabled system. A system that has an available PatchLink software agent, but a decision has been made by the system owner, and approved by the NASA CIO office, to not install the PatchLink software agent.

4. Patch Selection Criteria

Each vendor rates patches that are released for operating systems and applications. The most severe rating is normally marked critical. ERS will be used to report on all critical patches as determined by the vendors.

- Additional patches or report requests can be added as needed by the NASA CIO office or the CCITS office. The ASUS project team will coordinate with each Center PatchLink administrator on the additional patches or reports.
- Custom patches will be discussed during the ASUS TIM before deployment and reporting (example: CIS reporting, DST patches, etc).

5. Patch Removal Criteria

Patches are removed from the monthly reporting requirement once the patch has been superseded by the vendor. Patch deletion requirements are discussed during the ASUS TIM.

6. Reporting Schedule

The Agency ERS system will be used for the monthly compliance reporting that is required for PatchLink enabled systems. In addition, quarterly reporting will be required of waived systems that meet the definition in section three. The calendar for all patch reports is available at: <https://patches.ksc.nasa.gov/reports.php>.

7. Reporting Schedule for PatchLink Enabled Systems

All reporting for PatchLink enabled systems will be accomplished by the Agency ERS. The reports will be provided to the NASA CIO office on the second Monday of each month.

8. Reporting Schedule for Non-PatchLink Enabled Systems (Waivers)

Quarterly reporting for Non-PatchLink/ERS enabled (waivered) systems will be accomplished manually. The ASUS Team will provide a reporting schedule based on the Patch Management Baseline (PMB). The spreadsheet is available on the ASUS web site:

<http://patches.ksc.nasa.gov>.

Additionally, a quarterly patch compliance report is required for waivered systems and is synchronized with other FISMA reporting. It is due from each Center on the following schedule:

- Second Monday of December will report on the PMB for September, October and November.
- Second Monday of March will report on the PMB for December, January and February.
- Second Monday of June will report on the PMB for March, April, and May.
- Second Monday of September will report on the PMB for June, July, and August.

9. Manual Reporting from PatchLink Servers Unable to Utilize ERS

Agency PatchLink systems that are unable to connect to ERS are required to provide the same database snapshot information as the PatchLink enabled systems. Examples of manual reporting systems: air-gapped servers, or systems that are installed outside the continental United States.

These systems will install the ERS software module and schedule the creation of a database snapshot file on the second Monday of each month. This file will then be securely transferred to the ASUS project office and imported into the Agency ERS database.

 7-20-2007
Robert L. Binkley
Deputy Chief Information Officer for IT Security (Acting)