A BasisOnDemand.com White Paper

# WHITEPAPER ON SAP SECURITY PATCH IMPLEMENTATION

Helps you to analyze and define a robust strategy for implementing SAP Security Patches

by Prakash Palani
(Prakash.palani@basisondemand.com)

# Table of Contents

1. Introduction ..... 3
2. Security Notes / Patches – an Introduction ..... 3
3. Phases of Implementing Security Notes ..... 3
4. Define (Phase 1) ..... 4
5. Determine (Phase 2) ..... 6
6. Points to Take Home ..... 11
7. References : ..... 11

## 1. Introduction

This paper describes the approach that needs to be followed for applying SAP Security Patches for ABAP and Java based systems. It also indicates the various options those can help you to implement the security notes according to SAP best practices.

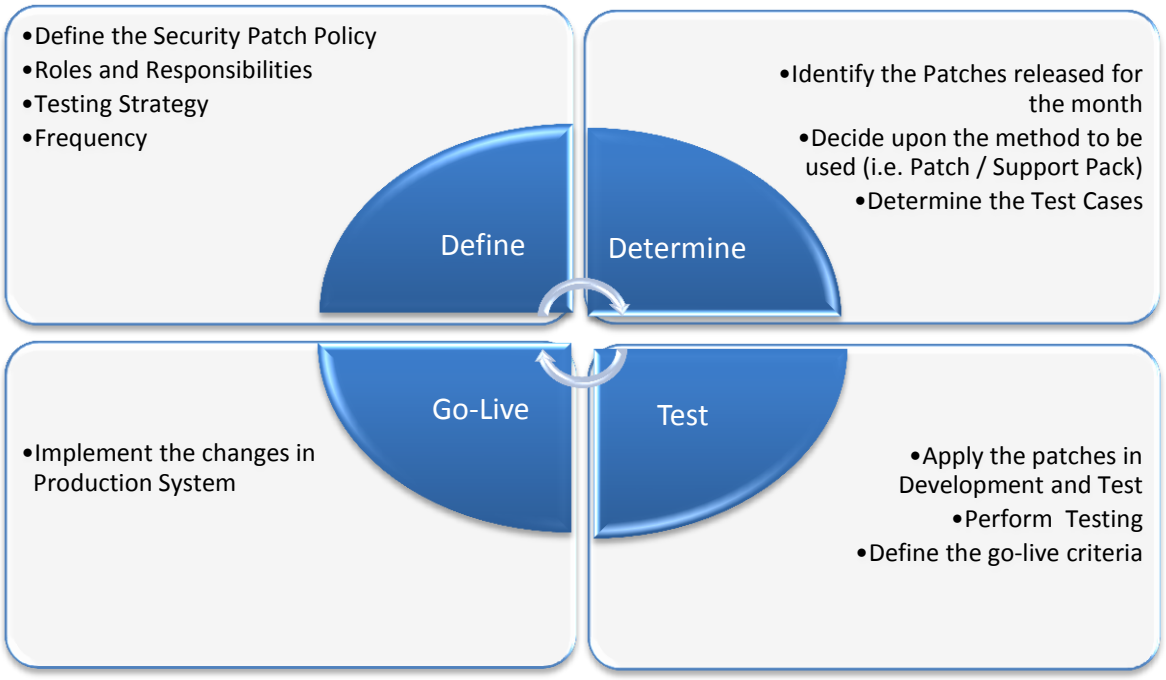
## 2. Security Notes / Patches – an Introduction

The SAP Security notes contain important security fixes for the SAP Netweaver Technology and SAP Business Suite applications. When a security note contains an ABAP correction, it can be applied to the SAP system by applying an OSS Note (using SNOTE) without applying the entire Support Package. This is often necessary to correct a specific issue that is impacting the business and cannot wait until the next time Support Packages are applied to the system. In some cases, security notes may contain corrections which need to be applied manually using development tools/configuration transactions.

In case of a Java Stack, it is delivered as a security patch (i.e. SCA files) which can be applied using JSPM/SDM in Java stack. Java patches will also be bundled with the support package and will be released as part of the next SP Stack release.

## 3. Phases of Implementing Security Notes

Implementing security patch is not a onetime process; rather it is a continuous process which should be implemented on a monthly/pre-defined interval basis. Like any other product vendor (i.e. Microsoft), SAP has come up with an approach of releasing the security notes on a specific day of a month, as an SAP user, it is imperative for any customer to align with the security recommendations from SAP. Below is the roadmap that we recommend to follow when dealing with the security patches. The same may vary based on the change management process of the customer.



This paper focuses on the first two phases of the security note implementation as the other phases are quite straight forward in nature as it involves applying OSS Notes and Java Patches.

## 4. Define (Phase 1)

Following sections will give necessary information on defining a robust security patch policy.

**Project Team**

Security Patch implementation is not something to be handled only by the Security/Basis consultants, it must be a joint effort with all the parties involved; any OSS Notes implementation requires impact analysis and testing, when it comes to security notes, one must perform detailed impact analysis, apply OSS note, make changes to the roles affected by the OSS Note implementation and extensive testing before moving it to production. If it needs to be done by a person who is not aware of the security processes in specific to the environment, it will lead to a massive failure. Hence it is imperative to identify and involve all the necessary team to have smooth ride on implementing security patches.

**Roles and Responsibilities**

*Identifying Security Patches* - It is the responsibility of security team to identify the security patches released for the month.

*Impact Analysis* - Respective business process owners are to perform the impact analysis based on the information collected in Security Notes and Patch Day and to come up with the mitigation plan to minimize the impact.

*Applying OSS Notes* - It is generally a responsibility of Basis Team to apply the security patches in ABAP (OSS Note) and Java (patch) based systems.

*Test* - Testing team must be involved in verifying the affected business processes.

*Go-Live* - Applying the notes (transport request) (or) the Java patches in production system are generally done by Basis Consultants.

**Frequency**

SAP releases the security patches on a **Second Tuesday** of every month, as a first step of the security notes implementation, it is recommended to analyze the security patches released for the month using http://service.sap.com/securitynotes. In addition to quicklink /securitynotes, you can get additional information on the released patches under /securitypatchday, this link gives little more information on the patches released for the month and the testing scenarios to be used after implementing the patches.

**Options to determine the applicable patches**

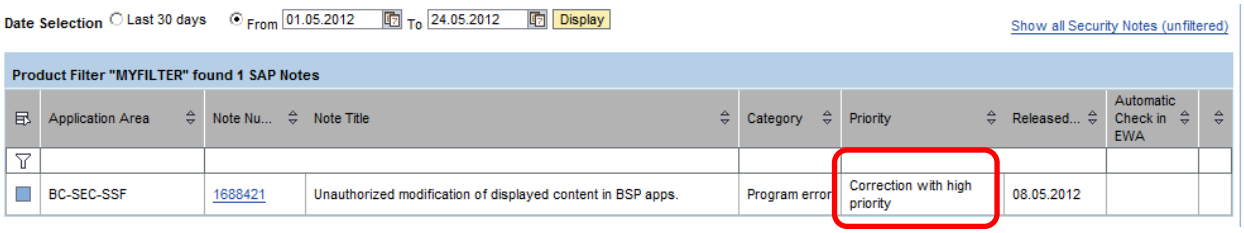
There are various ways to identify the security patches that are applicable to your system landscape as mentioned below; you may choose the option that is available and easier for your environment.

1. service.sap.com/securitynotes - > Security Notes Search
2. service.sap.com/securitynotes -> mySecurity Notes
3. Using Early Watch Alert / RSECNOTE – **Applicable only to ABAP stack**
4. Using Security Optimization Self Service – **Applicable only to ABAP stack**
5. Using SAP Solution Manager 7.1 - > System Recommendations
6. Searching in /notes -> using “Security is endangered” restriction

Detailed information on each of the above options is described under section Phase 2 – Determine (section 5).

**Identify the Implementation Method :**

Not all the patches are to be applied in a single go, one can decide upon the patches to be implemented based on the priority defined by SAP. Some patches may come with very high priority which needs to be applied in your landscape as soon as possible, in other cases, there may be patches released with high/medium priority which can be combined together with the half-yearly/yearly support pack upgrade strategy that you may follow in your environment. This is to help you to equip the team based on the priority.


Date Selection ○ Last 30 days ◉ From 01.05.2012 To 24.05.2012 Display Show all Security Notes (unfiltered)

Product Filter "MYFILTER" found 1 SAP Notes

| Application Area | Note Nu... | Note Title | Category | Priority | Released... | Automatic Check in EWA |
|---|---|---|---|---|---|---|
| BC-SEC-SSF | 1688421 | Unauthorized modification of displayed content in BSP apps. | Program error | Correction with high priority | 08.05.2012 | |

**Testing**

A testing strategy must be developed to ensure that Security Patches do not negatively impact business functionality. Testing should cover all business processes affected by the patch. Detailed information given in the Patch Day document can be used for identifying the areas to be tested.

The following are exemplary areas to be considered for the testing:

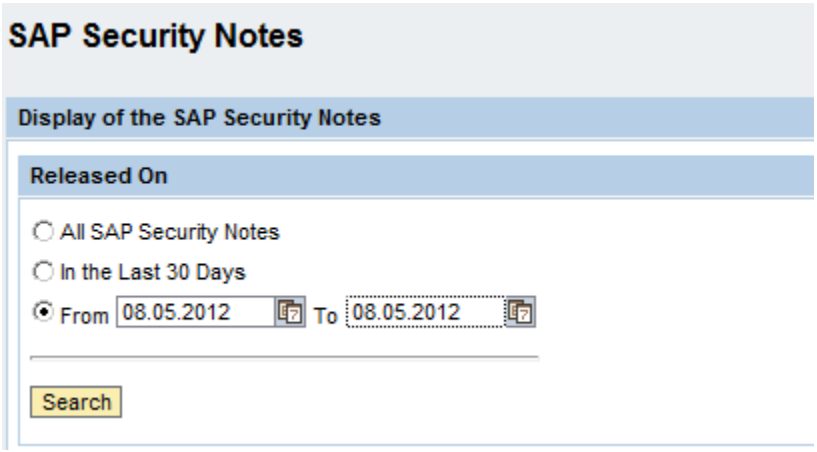
- Business Processes
- Interfaces
- Custom Developments

## 5. Determine (Phase 2)

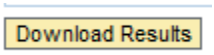
As mentioned in section 4, there are various methods available to determine the security notes/patches that are applicable to your environment. Following sections explains each of the options in detail.

***Option 1: Security Notes Search***


*Step 1 :* Search for the security notes with the selection criteria as Patch Day of the month. (i.e. second Tuesday of May)




*Step 2 :* Download the results into excel file and use your own filter criteria to identify the security notes that are applicable.



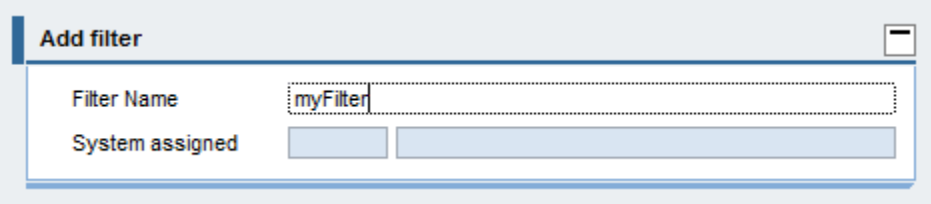

***Option 2: my Security Notes***


You can use this option to specifically search for a product or an SAP system available in your landscape, with this option, you can filter the systems/products maintained in system-data in marketplace and the components that you manually choose while defining the filter criteria.

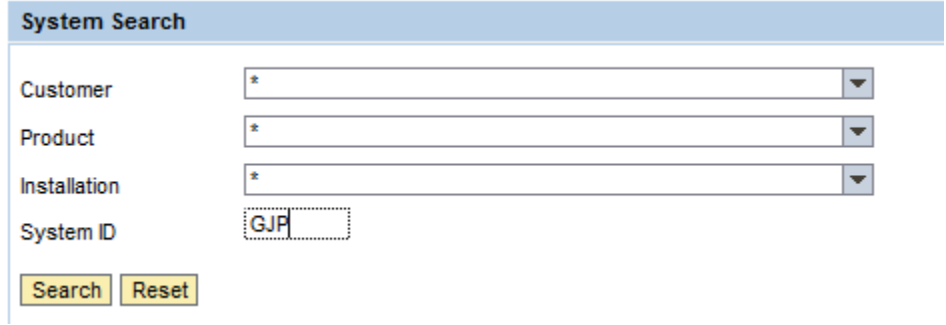
You must define the filter criteria once for each of the production system in your landscape, the same can be used for easily identifying the notes that are only relevant for that particular system. Hence you must pay attention to the filter criteria that you define, else it may lead to incomplete/wrong information.

*Step 1 : Add New Filter,*


Step 2 : Specify the Filter Name

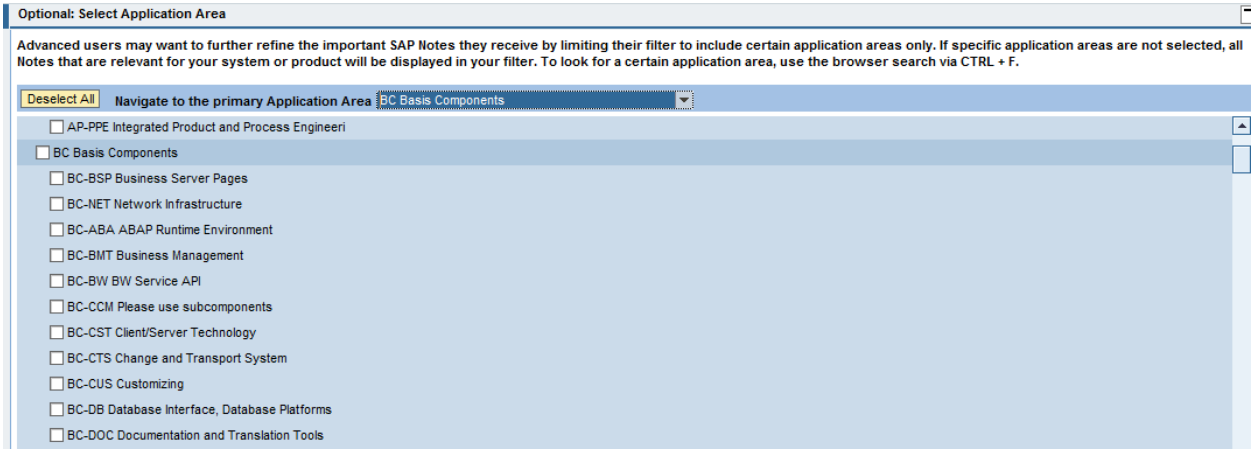



*Step 3 : Specify the SYSTEM ID for which you would like to get the security patch information*

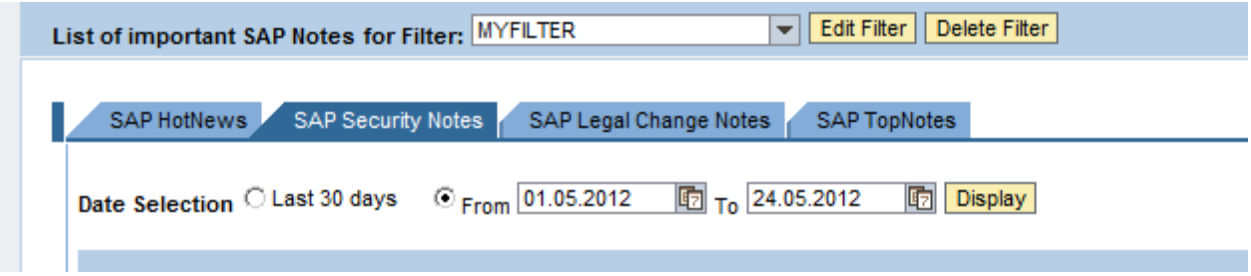



*Step 4 : Choose the System ID and continue*

*Step 5 : Advanced users may further refine the filter according to the components used.*



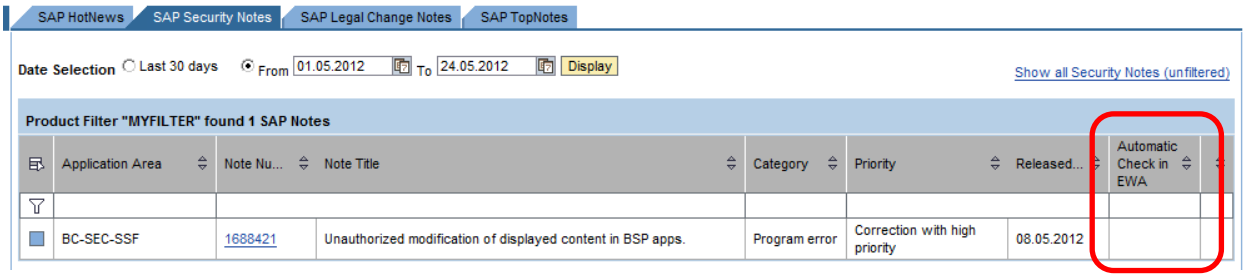
You are done with the filter creation; you can use the created filter every month to get the list of notes applicable for your system.




***Option 3: Using Early Watch Alert / RSECNOTE***

Since the security patches are released on the second Tuesday of every month, you can schedule Early Watch sessions to run every second Wednesday of every month, this will help to automatically identify the missing security notes as part of EWA sessions. Early Watch Alert will only indicate that there are missing security notes in the satellite system, in order to get the actual list, you must use transaction ST13 -> RSECNOTE to identify the complete list of missing security notes.

A most important disadvantage is that, only the notes which are marked as "Automatically Checked in EWA" (under /securitynotes quicklink) will be validated by EWA / RSECNOTE, hence it is imperative to use the manual options suggested in option 1 / option 2 in this document.



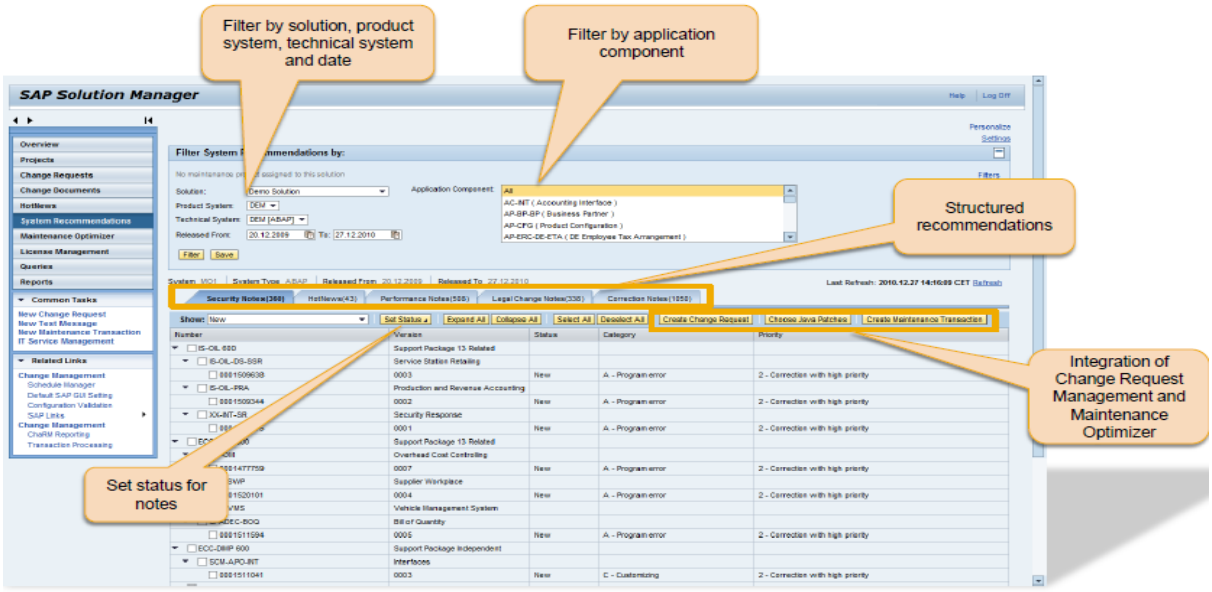

***Option 4 : Security Optimization Self Service (SOSS)***

SOSS is designed to verify and improve the security of the SAP system of customers by identifying potential security issues and giving recommendations on how to improve the security of the system. The same can be performed with the help of SAP Solution Manager 7.01. Please note that SOSS reports only the missing security notes of an ABAP stack, but does not help to identify the missing security patches of Java Stack. For more information, please refer to http://service.sap.com/SOS

**Option 5: System Recommendations functionality from Solution Manager 7.1 (Recommended Approach)**

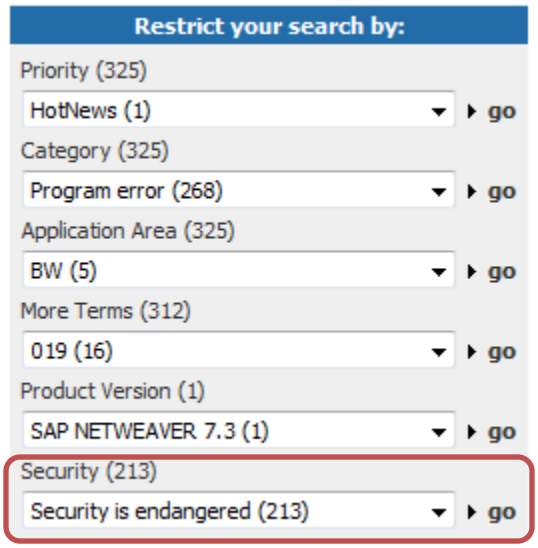
As of SM 7.1, SAP has introduced a functionality called “System Recommendations”, this functionality provides detailed information on SAP notes that are to be implemented for a particular system. The same is calculated based on the actual status of the system (i.e. applied notes ***vs*** new notes).

You can select a system to be checked which in turn will connect to SAP AG to calculate the delta information, then the same is sent back to the solution manager to calculate the actual status of the notes.



***Option 6: Using /notes with restriction "Security is endangered"***

You may also perform a generic search for SAP Security Notes using specific keywords under quicklink http://service.sap.com/notes. In order to get the notes that are relevant to SAP security, you must further restrict the search criteria using the topic Security as indicated below (Left side of the search result screen).




You can use the below keywords to narrow down your search for Security Notes.

| Topic | Keyword to be used in search |
|---|---|
| Cross Site Scripting | XSS |
| Cross Domain Redirection | Cross-domain redirection |
| Cross-site request forgery | XSRF |
| Information Disclosure | \|Information Disclosure" |
| Buffer Overflows | RCE, "Buffer Overflow" |
| SQL Injection | SQL Injection |
| Remote Termination | Memory Corruption |
| Denial of Service | DoS |
| Hard-coded credentials | Credentials, "hard-coded" |
| Directory Traversal | Directory Traversal |
| Code Injection | Code Injection |
| Missing authorization | authorization, "check" |

## 6. Points to Take Home

- Security Patch Implementation is not just a task of security/basis administrator
- SAP recommends making use of “System Recommendations” functionality from Solution Manager 7.10
- Test! Test! Test! It is the key to success!
- Make sure to continuously update the security patches
- RSECNOTE / EWA does not give complete information on the missing OSS Notes, you must still identify the security notes which are not identified by RSECNOTE/EWA
- For Java based systems, EWA/RSECNOTE/SOSS will not be useful, hence it is recommended to use “System Recommendations” from Solution Manager 7.10

## 7. References :

http://service .sap.com/securitynotes
http://service.sap.com/securitypatchday
http://service.sap.com/securitynoteFAQ