LAYER SEVEN SECURITY

SECURITY PATCHING FOR SAP SOLUTIONS

BEST PRACTICES FOR DISCOVERING, ANALYZING AND IMPLEMENTING SAP SECURITY NOTES

WHITE PAPER

SECURITY PATCHING FOR SAP SOLUTIONS

BEST PRACTICES FOR DISCOVERING, ANALYZING AND IMPLEMENTING SAP SECURITY NOTES

CONTENTS

INTRODUCTION

The risk of unpatched systems is continuously reported as one of the top three threats to SAP systems in every survey of SAP customers performed by SAPinsider since 2021. Keeping up with SAP patches and updates is reported as the first or second greatest security challenge confronted by customers in each year between 2021- 2023. Regularly implementing notes and patches is reported as the most significant action performed by organizations to secure their SAP solutions.

Regularly patching SAP systems is the single most important action you can take to secure business-critical SAP applications from cyber threats. Despite concerns related to zero-day vulnerabilities, every known SAP exploit has targeted existing vulnerabilities for a which a patch was readily available from SAP. There is no evidence of the exploitation of zero-day vulnerabilities for SAP applications. However, there is a wealth of evidence for the exploitation of known vulnerabilities that have been fully patched by SAP.

This includes well-known SAP vulnerabilities such as ICMAD, RECON and 10KBLAZE. Security notes 3123396 and 3123427 patch for ICMAD. Note 2934135 secures against RECON exploits. Protection against 10KBLAZE can be applied through notes 1408081, 821875, and 1421005. Some the notes for 10KBLAZE have been available since 2006. This is 13 years before CISA released an alert for the exploits.

Organizations take an average of three months to implement hot news notes for critical SAP vulnerabilities. Yet threat actors can weaponize SAP vulnerabilities within 72 hours of a patch release. Therefore, it is important to minimize the window of opportunity for attackers by rapidly discovering, analyzing and implementing SAP security notes.

Based on the findings of the surveys since 2021, it is clear that security patching is regarded by SAP customers as the most important action they undertake to protect their SAP systems from cyber threats and also the area they experience the greatest challenge. According to customers, the challenge is due to several factors. This includes the overwhelming volume of notes, the effort related to validating the relevancy of notes identified by SAP solutions, difficulties related to prioritizing notes, a reluctance to apply patches that could impact system availability, issues related to scheduling downtime for maintenance often due to competing business priorities, insufficient resources to apply notes, and the challenge of validating whether patches are correctly applied.

This guide provides clear and practical recommendations to overcome every one of the challenges to successfully patching SAP systems. Based on SAP guidance and best practices observed by Layer Seven Security from engagements spanning more than a decade, the paper addresses each of the issues reported in the surveys. We trust that the implementation of the recommendations in this guide will enable SAP customers to overcome one of the most persistent challenges to securing their SAP systems and address the most significant cybersecurity threat to SAP solutions.

[1] Cybersecurity Threats to SAP Systems, SAPinsider, 2021 - 2023

HIGH VOLUME OF SECURITY NOTES

Security notes are applicable to specific software components installed in systems. The emphasis is on installed components, not used components. Since installed components are part of the attack surface in an SAP system, they must be patched regardless of usage.

Since security notes are applicable to specific system types with the relevant installed software components, the challenge of dealing with the high volume of notes released by SAP on Patch Tuesday (the second Tuesday of each month) can be managed by automating the discovery of relevant notes based on available system types in your SAP landscape and the installed software components and versions within the systems.

There are several options for automating the discovery of relevant SAP security notes. Maintenance Planner is available in the SAP Support Portal and accessed using at https://support.sap.com/mopz. It calculates relevant notes based on system and software information sourced and synchronized daily from the Landscape Management Database (LMDB) in SAP Solution Manager within customer SAP landscapes. The information in the LMDB is derived directly from the SAP System Landscape Directory (SLD) in each landscape.

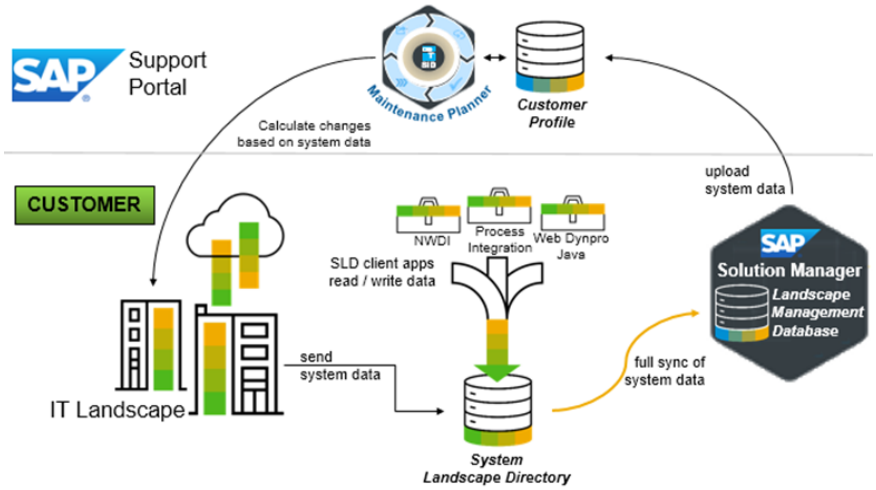

Figure 1.1 SAP Maintenance Planner – Architecture

System and software information sourced from the LMDB can be reviewed using the Explore Systems tile in the Plan and Execute section of Maintenance Planner.

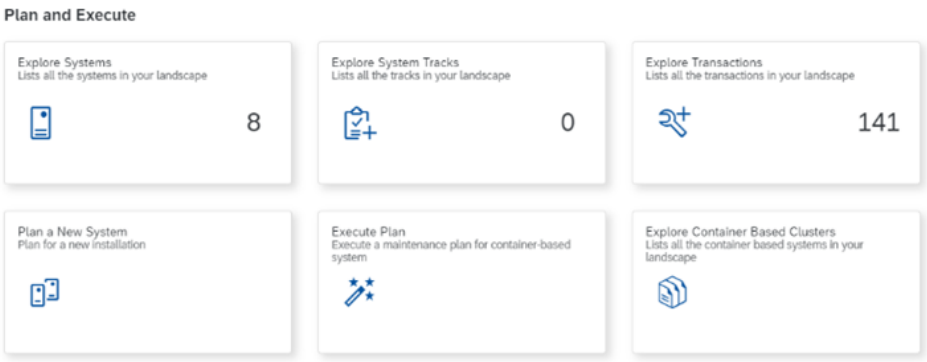

Figure 1.2 SAP Maintenance Planner – Plan and Execute

Explore Systems provides detailed software information for each system such as product versions, components and stack levels, as well as tracks and dependencies. Tracks are used to group related systems and streamline maintenance.

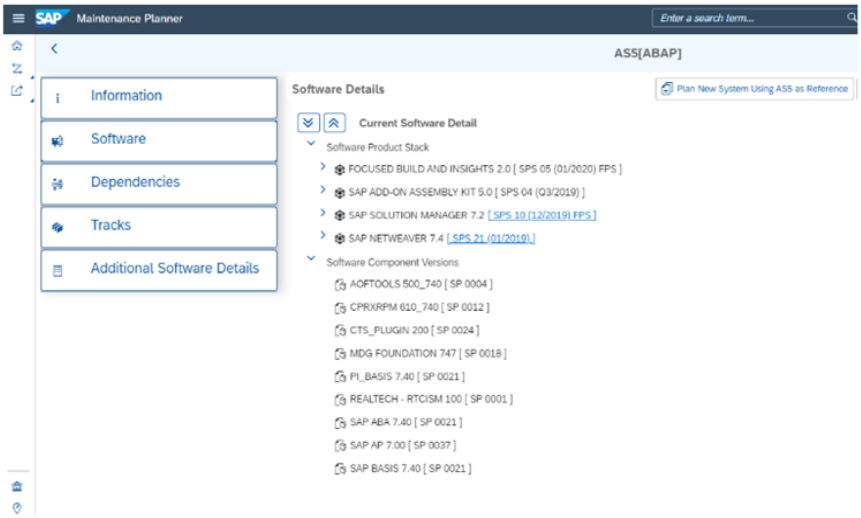

Figure 1.3 SAP Maintenance Planner – Explore Systems

Maintenance Planner identifies products that are out of maintenance, third-party add-ons installed in SAP systems, and inconsistencies between displayed software components and installed components in systems. Upgrade Dependency Analyzer (UDA) is integrated with Maintenance Planner to help identify the impact of maintenance tasks in dependant systems. Maintenance Planner identifies and downloads the required software packages for planned upgrades or new systems. Maintenance Planner calculates and displays recommended notes for systems in each landscape. The notes are analyzed and managed using the View Recommended Notes tile. It supports searching, filtering, grouping, sorting, and exporting of results. The Calculate Notes option displays relevant notes for selected systems. Notes are grouped by category including Security. You can select a note from the available categories to view the details. CVE, CVSS and vector information is included for SAP Security Notes.

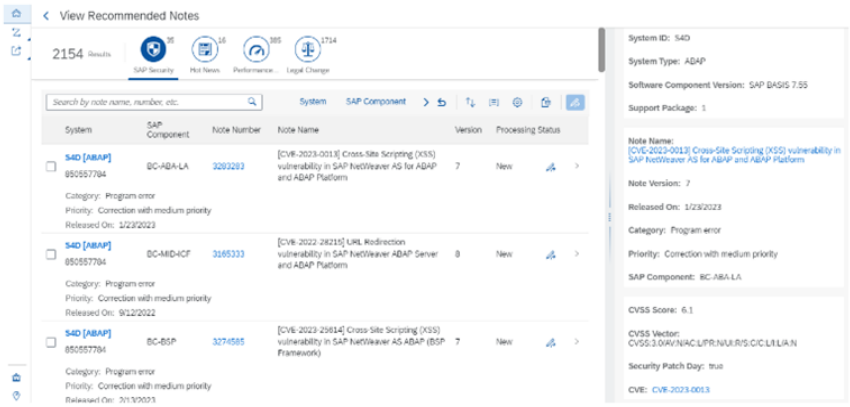

Figure 1.4 SAP Maintenance Planner – View Recommended Notes

Maintenance Planner can track the implementation lifecycle of notes using the Processing Status option. The following values are supported for the option:

Transferring: Note is transferred for implementation

In Progress: Note implementation is in progress
Not Relevant: Invalid or irrelevant note for the system

A Comments field is also included for users to provide additional information related to the processing status of each note.

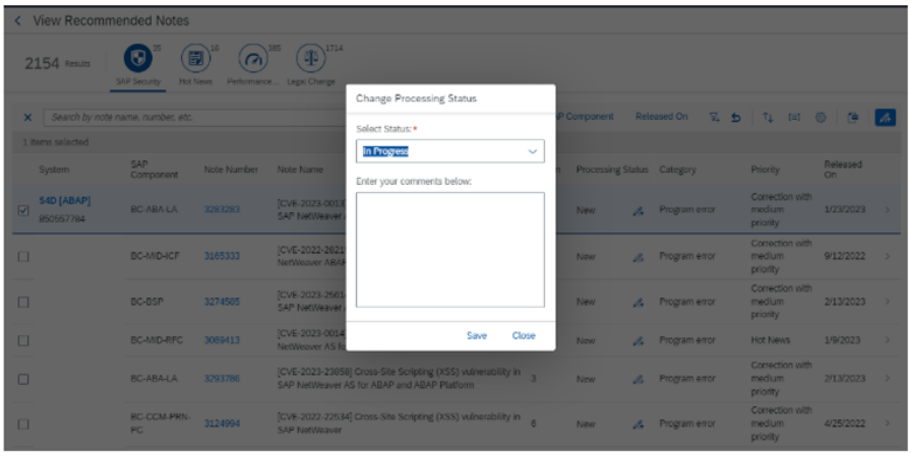

Figure 1.5 SAP Maintenance Planner – Change Processing Status

Security notes with automated corrections can be applied individually or through support pack (SP) upgrades. As discussed in later sections, SP upgrades are recommended for applying low and medium priority security notes. The SAP EarlyWatch Report (EWA) can be used to identify outdated Support Packages for systems. EWA can be accessed from the Launchpad for SAP ONE Support or SAP for Me. It is also available in the SAP Engagement and Service Delivery Work Center in SAP Solution Manager.

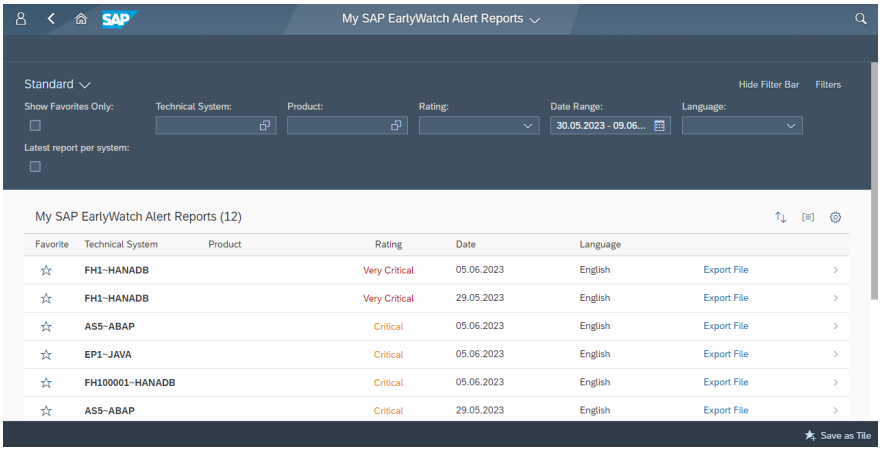

Figure 1.6 SAP Solution Manager – EarlyWatch Reports

Figure 1.7 SAP Solution Manager – EarlyWatch Results

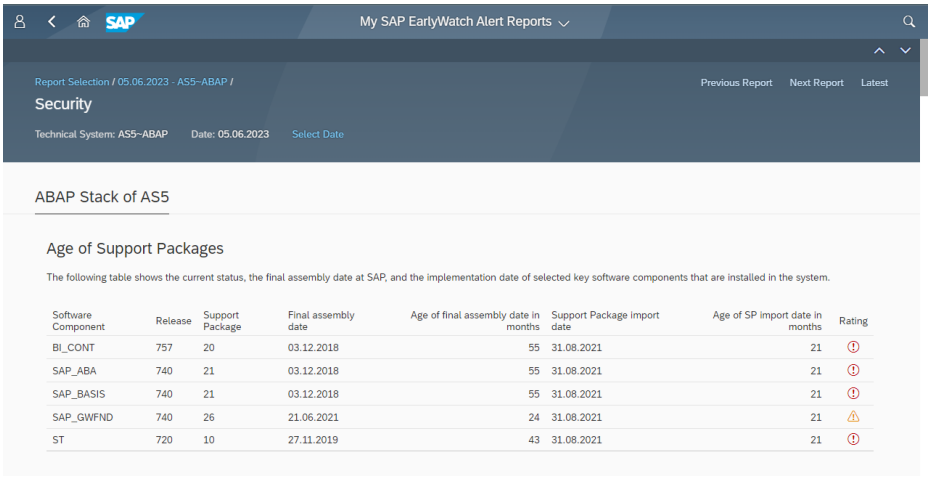

Figure 1.8 SAP Solution Manager – Support Packages

System Recommendations (SysRec) in SAP Solution Manager provides the most comprehensive solution for discovering relevant security notes for SAP systems. It is the only solution that supports the full lifecycle management of SAP security notes. SysRec is a standard application in SAP Solution Manager, recommended by SAP for patch management. It is automatically enabled during the installation and setup of Solution Manager.

Similar to the Maintenance Planner, SysRec calculates notes based on system and software information stored in the LMDB. The calculation is performed weekly by default but can be changed to a daily check for new notes. This will notify SAP customers as soon as a new note is released.

SysRec has several advantages over Maintenance Planner for notes discovery. Unlike Maintenance Planner, SysRec calculates notes for SAP platforms including databases and operating systems and standalone components. This includes HANA, ASE, SAProuter and the Web Dispatcher. It also analyzes the implementation status of notes for ABAP systems and removes notes with automated corrections that have been fully implemented from the results. For notes with manual corrections, SysRec supports the addition of custom status options to tag and remove implemented notes. In both cases, this reduces the volume of security notes by removing patches that have already been applied.

SysRec also has the advantage of displaying prerequisite and side-effect notes for calculated results. Prerequisite notes are required before implementing corrections and side-effect notes are recommended to counter known issues with implementing the corrections.

SysRec supports more advanced filtering and sorting for security notes than Maintenance Planner. This includes filtering results to identify kernel-dependant notes and notes that can be applied using available support packages. The relevant support package numbers are included in SysRec.

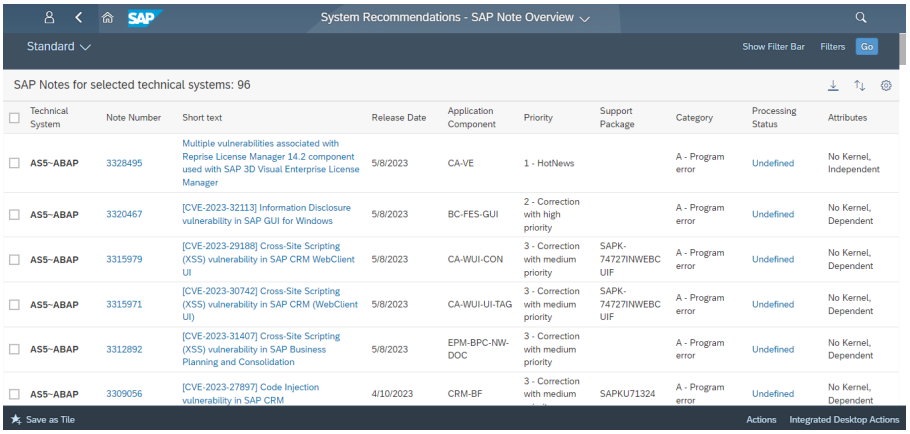

Figure 1.9 SAP Solution Manager – System Recommendations

Since SysRec is widely used by SAP administrators to manage not only SAP security notes but also correction, legal, performance and other notes, it is also recommended for internal security groups. This will avoid inconsistencies that can arise when SAP security groups rely on third party solutions to discover security notes. The results of third party tools may not align with the results calculated by SysRec. SAP Basis administrators are inclined to trust the results of SAP-delivered applications such as SysRec over non-SAP solutions. This can lead to disputes and delays within organizations as SAP Basis and security groups fail to align on the notes that should be implemented. The risk is avoided when the groups share the same platform and therefore organizations are aligned on the relevant security notes that need to be applied.

For customers using SAP Focused Run for notes discovery, security notes can be calculated using Configuration and Security Analytics (CSA). SAP releases XML policies after Patch Tuesday in each month containing the rules to validate the relevancy of newly released security notes for systems. The validation is based on the availability of relevant software components and the implementation status of notes. Software component information for each system is stored in the Configuration and Change Database (CCDB) and updated regularly. The XML policies for each month should be added to a composite policy for all security notes to identify missing patches covering a longer period of time.

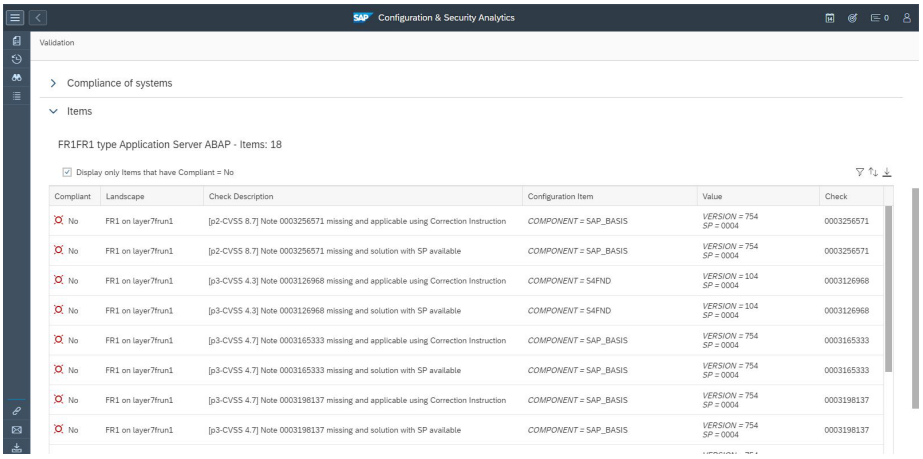

Figure 1.10 SAP Focused Run – Configuration and Security Analytics

Recommendations:

Automate the Discovery of Relevant SAP Security Notes using Maintenance Planner, Solution Manager, or Focused Run

IRRELEVANT SECURITY NOTES

Maintenance Planner, System Recommendations in SAP Solution Manager, and CSA in SAP Focused Run calculate applicable notes based on the availability of relevant software components in systems. Most security notes released by SAP include software component information. However, some notes do not include details of impacted software components. This can lead to false positives in the security notes calculated for systems. Reviewing and validating security notes to identify and remove false positives can be time-consuming and may delay the implementation of required corrections. This is especially an issue for large SAP landscapes with a high volume of systems.

The Cybersecurity Extension for SAP (CES) automatically discovers potential false positive security notes calculated by SAP applications such as System Recommendations and CSA. CES analyzes notes based on the availability of relevant application components. The status of notes that are related to application components that are not installed in target systems is changed to Irrelevant and removed from the results calculated by SysRec. This dramatically improves the quality and reliability of security notes calculated for SAP systems and eliminates the manual effort involved in validating results. It also enables organizations to apply corrections more rapidly and therefore minimize the window of opportunity for threat actors to exploit SAP vulnerabilities.

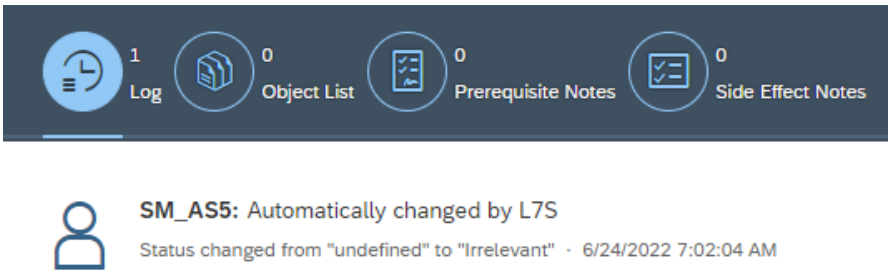

Figure 2.1 SAP Solution Manager – System Recommendations – Change Log

Irrelevant application components for databases and operating systems can be hidden using the customizing table AGSSR_OSDB for System Recommendations. The table can be maintained with transaction SM30 in SAP Solution Manager. Relevant components can be set to Active and irrelevant components can be designated as Inactive. Notes for inactive components will not be displayed in System Recommendations.

Recommendations:

Implement the Cybersecurity Extension for SAP to automatically validate calculated security notes and remove false positives

Maintain table AGSSR_OSDB in SAP Solution Manager for System Recommendations to set active and inactive DB and OS application components

PRIORITIZING SECURITY NOTES

Based on the volume of security notes released between 2021 – 2023, there are an average of 16 notes released by SAP each Patch Tuesday. Since notes are applied in each system, a single SAP note can be applicable for multiple systems across several environments in SAP landscapes. The effort required to analyze and implement the corrections for required notes increases precipitously with the number of environments and systems in each landscape.

This effort can be managed by prioritizing the implementation of security notes based on the risk of the underlying vulnerabilities addressed by notes. Security notes are categorized using a priority scale of hot news (critical), high, medium and low. The priority of a note is based on the CVSS score of the related CVE for each note.

Low and medium priority notes for minor CVEs account for approximately 65 percent of security notes released between 2021 – 2023. These notes can be implemented through support packages if the notes include automated corrections and organizations perform regular SP upgrades for systems. This can reduce the volume of required notes by up to two thirds. Medium and low priority security notes with automated corrections and available support packages can be identified using filters in System Recommendations. The status of the notes can be changed to Postponed to indicate that the corrections will be applied through the implementation of the relevant support package.

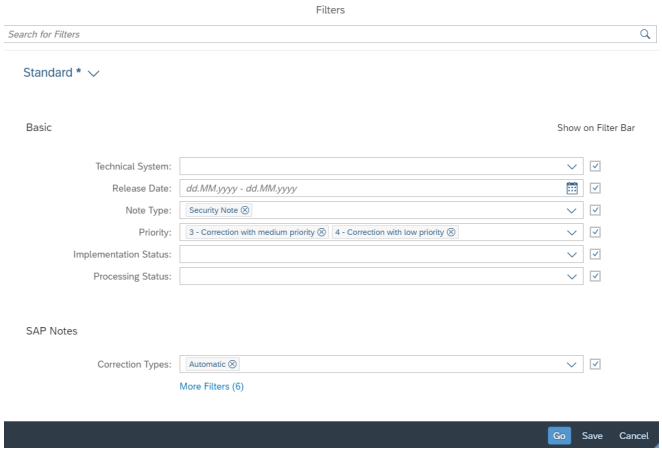

Figure 3.1 SAP Solution Manager – System Recommendations – Filters

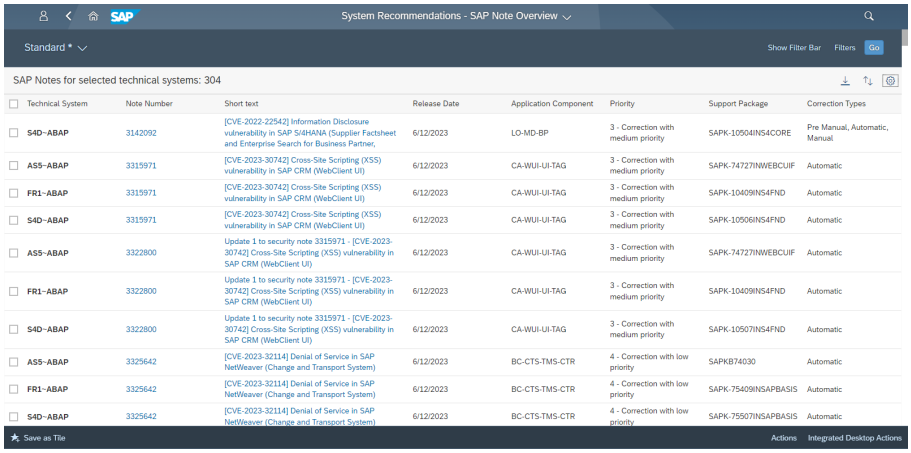

Figure 3.2 SAP Solution Manager – System Recommendations – Results for Medium and Low Priority Security Notes with Automatic Corrections and Support Packages

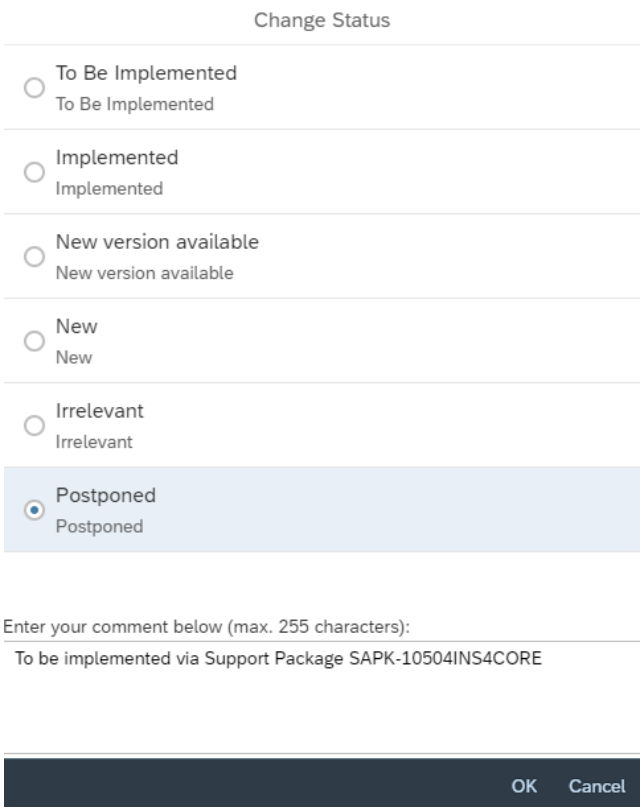

Figure 3.3 SAP Solution Manager – System Recommendations – Note Status

Hot news security notes should be prioritized for implementation within 30 days of the release date. Corrections for high priority security notes should be applied within 90 days of the release date. Hot news and high priority security notes account for approximately 15 and 20 percent, respectively, of the security notes released by SAP.

Recommendations:

Implement Hot News Security Notes within 30 Days
Implement High Priority Security Notes within 90 Days
Implement Low and Medium Security Notes using Support Packages

MAINTAINING SYSTEM AVAILABILITY AND INTEGRITY

SAP solutions include numerous software and application components, as well as thousands of technical objects such as function modules, methods, and programs. Security notes can impact the availability and performance of components and objects in systems. Therefore, identifying the impact of notes before they are applied is vital, especially for SAP solutions that require high availability. Insufficient information to support the identification and testing of areas impacted by security notes is often cited as the root cause of long patch cycles that delay the implementation of security notes.

This can be addressed by referring to the Object List for each security note in System Recommendations. The Object List identifies the specific objects impacted by the note. It also provides usage counts for the objects. Usage counts are sourced from Usage and Procedure Logging (UPL) and the ABAP Call Monitor (SCMON) in SAP Solution Manager. This information enables SAP administrators to determine the scope and extent of testing required for security notes. Notes impacting many objects with high usage counts may require detailed integration or regression testing. Conversely, notes impacting few objects with low usage counts indicate that customers may be able to employ less complex and more rapid test methods such as smoke tests.

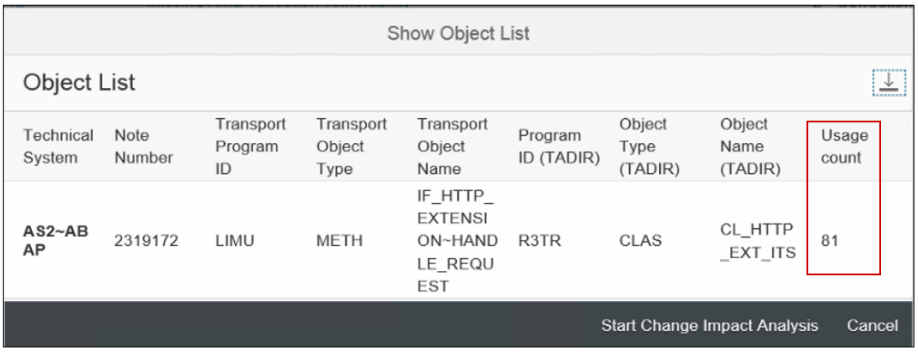

Figure 4.1 SAP Solution Manager – System Recommendations – Object List

Business processes impacted by security notes can be identified using the option Start Change Impact Analysis for selected notes from Integrated Desktop Actions in System Recommendations. This option integrates with Business Process Change Analyzer (BPCA) in SAP Solution Manager. Business process information is maintained in Solution Documentation. The results of the change impact analysis can be integrated with Test Suite in Solution Manager for selecting and executing custom and SAP-delivered test plans covering impacted areas.

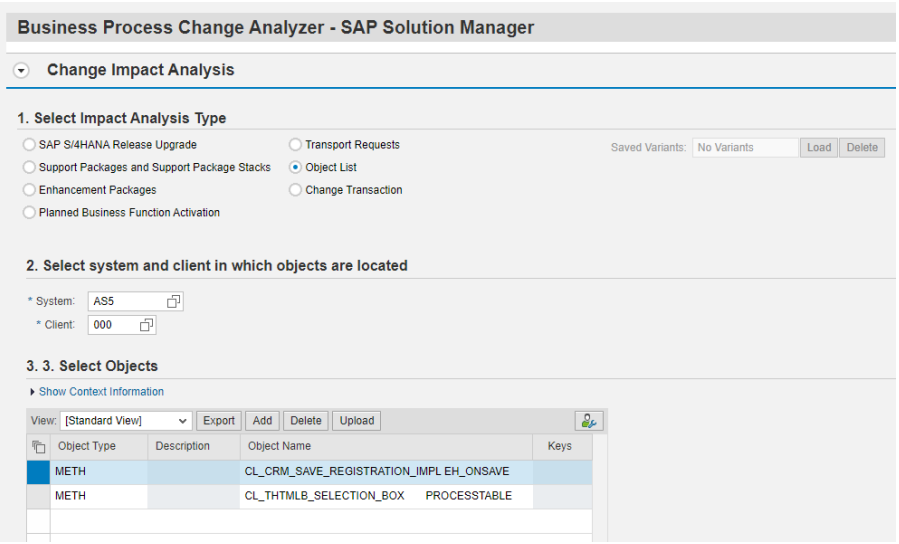

Figure 4.2 SAP Solution Manager – System Recommendations – Change Impact Analysis

Recommendations:

Analyze the Object List for Security Notes in System Recommendations

Perform Change Impact Analysis for Security Notes in System Recommendations

SCHEDULING DOWNTIME FOR SECURITY PATCHING

The implementation of security notes via SNOTE in ABAP systems does not typically require a system restart and therefore there is no need to schedule downtime for security patching. However, restarts are required for notes that involve kernel upgrades. They are also required for HANA, Java and other systems when upgrading software components, unless they are revision updates.

This can be a significant challenge since SAP solutions typically need to maintain a high level of availability. The implementation of security notes should be scheduled at the same time as other maintenance tasks to minimize the downtime. Maintenance windows should be scheduled using Work Mode Management in SAP Solution Manager. Scheduling downtime in Work Mode Management will supress availability alerts and ensure that downtimes do not impact SLA targets for availability.

Change Request Management (ChaRM) in SAP Solution Manager should be used to request, approve and track the implementation of security notes. ChaRM requests can be created for required security notes directly in System Recommendations using the option Create Request for Change. The requests can be migrated progressively through system environments based on the integration between ChaRM and the Transport Management System (TMS).

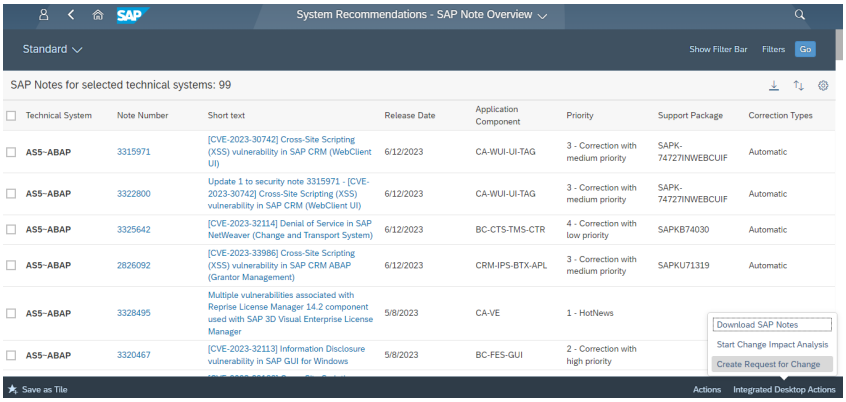

Figure 5.1 SAP Solution Manager – System Recommendations – Create Request for Change

Recommendations:

Include the implementation of security notes in maintenance work modes maintained using Work Mode Management in SAP Solution Manager

Request and track the implementation of security notes using Change Request Management (ChaRM) in SAP Solution Manager

INSUFFICIENT RESOURCES TO APPLY SECURITY NOTES

The root cause of resource constraints related to analyzing and applying SAP security notes is often inefficient patching procedures. Patching procedures that rely on manual methods or fail to focus on critical and high priority notes will require more effort and therefore consume more resources than procedures that rely on automated methods and use a prioritized approach for notes. The effective use of System Recommendations in combination with the Cybersecurity Extension for SAP, Change Impact Analysis, Test Suite, Work Mode Management, and Change Release Management will reduce resource requirements and streamline patching processes. The efficiency gains realized through automation can be increased by concentrating patching efforts on hot news and high priority notes and excluding medium and low medium priority notes. The latter account for approximately two-thirds of security notes.

Recommendations:

Automate Patching Procedures

Prioritize Hot News and High Priority Security Notes

VALIDATING THE IMPLEMENTATION OF SECURITY NOTES

System Recommendations analyzes the implementation status of notes when calculating relevant security notes for ABAP systems. Notes can have the following implementation status values:

1. Incompletely implemented - Not all the relevant correction instructions have been implemented, or some correction instructions have only been partly implemented. The objects that need to be corrected are inconsistent. You must therefore implement this SAP Note in your system again.

2. Obsolete version implemented - SAP has corrected an SAP Note that contained errors. Implement this note in your system again.

3. Can be implemented - The SAP Note contains correction instructions that you may need to implement in your system.

4. Implemented completely - The corrections in the SAP Note have been implemented completely in your system. No action is required.

5. Cannot be implemented - The SAP Note does not contain any correction instructions that you can implement in your system. No action is required.

6. Deprecated – After you implemented the corrections in the Note, you imported a Support Package that also contains these corrections. The errors have now been removed.

Notes with values (4), (5) or (6) are considered implemented or not relevant and are automatically removed from the calculated results in SysRec.

Kernel notes and notes for HANA and Java systems are calculated by SysRec based on the versions and patch levels of installed kernels and software components. This information is sourced from the LMDB. The LMDB is periodically synchronized with the SLD. Therefore, security notes that were previously calculated as relevant for HANA and Java systems should be automatically removed in SysRec once the software information is updated in the LMDB to include the required versions, SP level or patch level. A manual refresh can also be triggered using the option Refresh Technical System from SLD in the System Overview section of the LMDB.

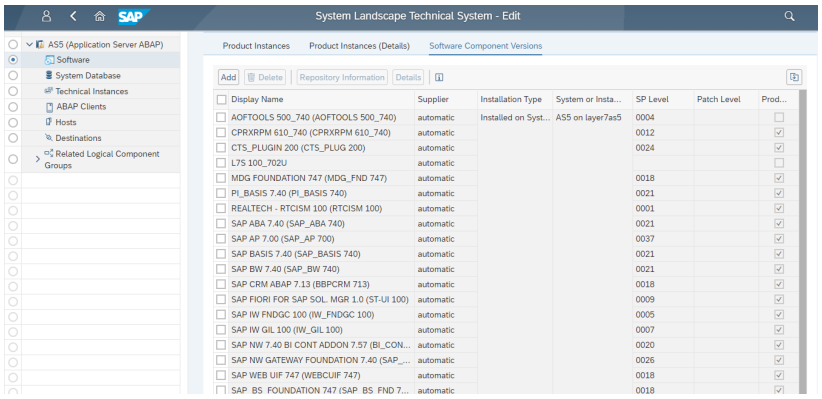

Figure 7.1 SAP Solution Manager – LMDB – Software Components

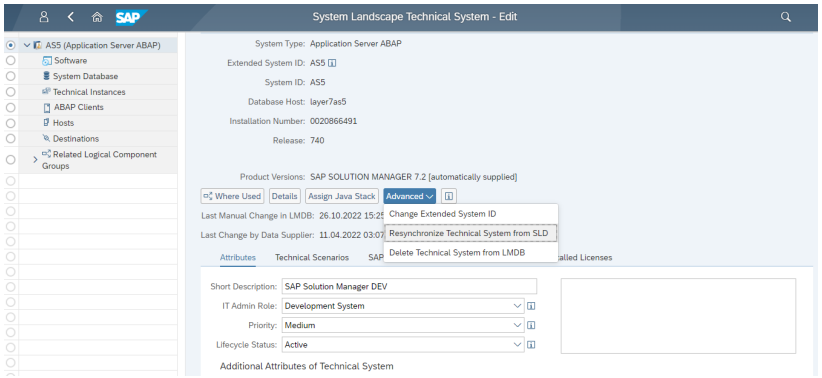

Figure 7.2 SAP Solution Manager – LMDB – SLD Synchronization

Notes with manual corrections can be labelled as Implemented using the Status option in System Recommendations. A status option for implemented notes can be added using the customizing table AGSSR_STATUS maintained via transaction SM30 in SAP Solution Manager. Security notes with the status value Implemented will be excluded from the results in SysRec based on the default filters.

The Cybersecurity Extension for SAP tracks and reports security notes implemented in SAP systems. Notes implemented within the last 90 days are reported in the Vulnerability Report and include details of the note number, version, implementation status, and implementation date. The results can be exported for offline analysis and reporting.

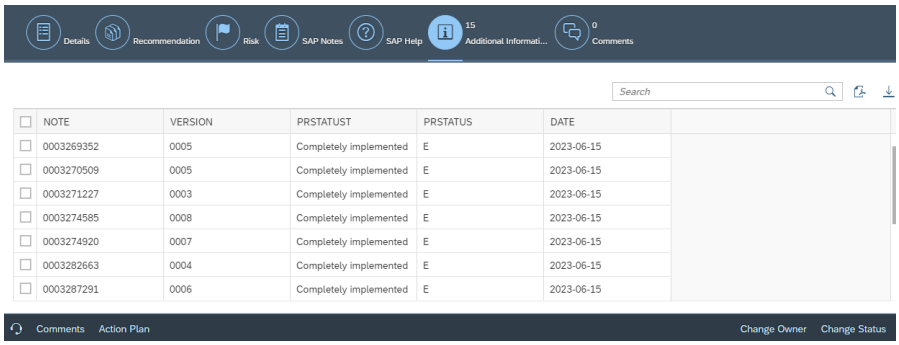

Figure 7.3 Cybersecurity Extension for SAP – Vulnerability Report – Implemented Notes

LAYER SEVEN SECURITY

Layer Seven Security is an SAP Partner and an industry leader in the provision of security solutions and services for SAP platforms. The company is recognized as one of the Top Ten SAP Solution Providers of 2018, Top 25 Cybersecurity Companies of 2020, and Top Threat Intelligence Solution Providers 2023.

Layer Seven Security's SAP-certified Cybersecurity Extension for SAP delivers advanced vulnerability management, threat detection and custom code security to secure SAP systems from cyber attack

CONTACT US

www.layersevensecurity.com
info@layersevensecurity.com