

# SAP Patch Days, Do you have a Process Around it?

Gaurav Singh  
Manager, SAP Cyber Security

Under Armour



**Sponsored by: Iron  
Man 😊**

# Agenda

- What are SAP Patch Days?
- Which Team is Accountable for SAP Patch Day? Security or Basis?
- Where to Start?
- Have a Process, to begin with, along with RACI
- Start with Knowing where you stand.
- Don't try to remediate all Vulnerabilities at once; you will fail.
- Focus on fixing Critical Vulnerabilities first.
- Do you have a tool to scan your SAP systems for vulnerabilities?
- On Prem Vs. Rise with SAP, Shared responsibility
- Go Beyond Patch days and Build SAP Vulnerability Management Program

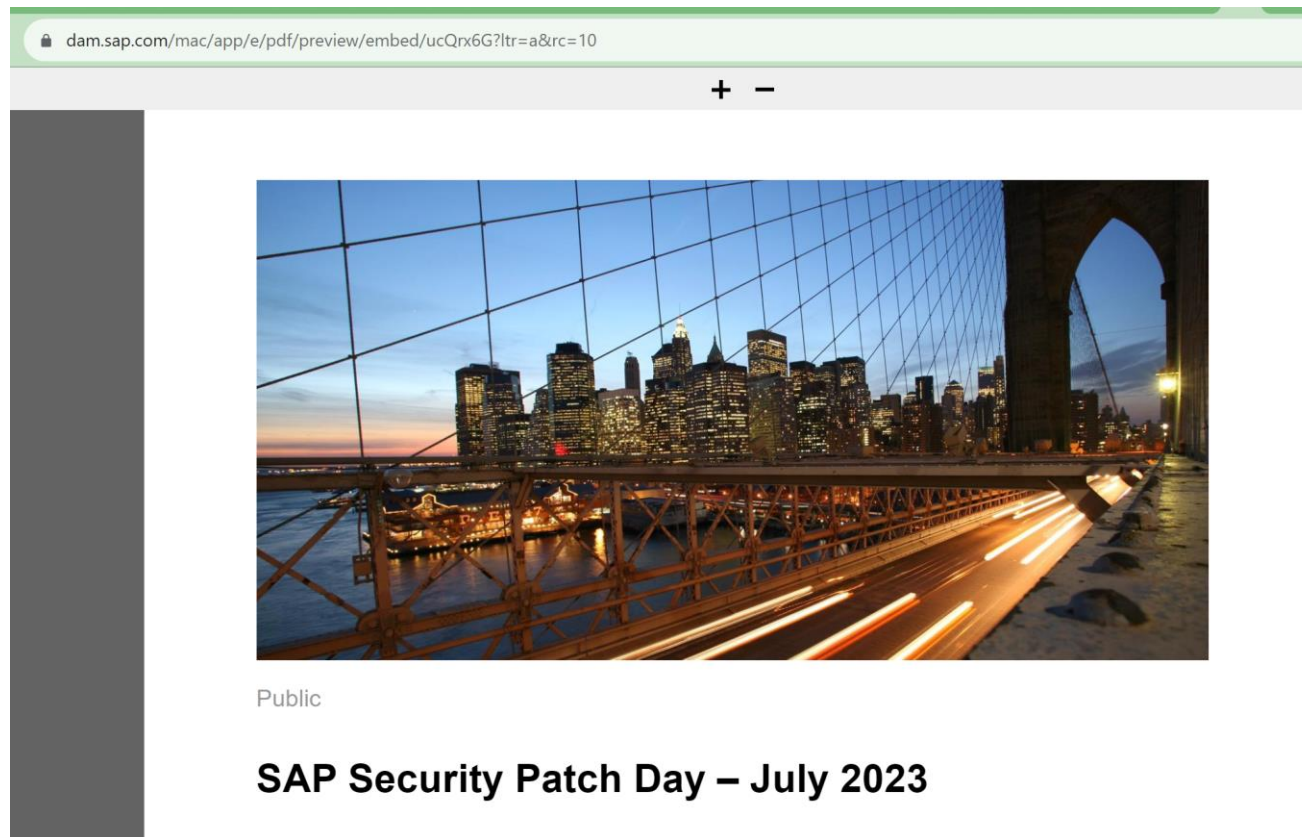
# What are SAP Patch Days?

- As with other major software vendors, SAP releases fixes/patches for new Vulnerabilities every 2nd Tuesday of the month.
- As SAP Security and Basis community, there needs to be clear ownership for SAP Customers and SAP Services companies.
- This is one area most of the SAP Security team ignores and doesn't focus on, whereas the Basis team limits themselves to SP upgrades which may not be happening as frequently as we would like to happen, which end up with SAP ecosystems with known critical and High vulnerabilities, which in turn can cause of the breach.

# What are SAP Patch Days?

SAP Security Patch Day URL-

<https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10>



# Who's Accountable for it?

- As SAP Security and Basis community, there needs to be clear ownership for SAP Customers and SAP Services companies.
- This is one area most of the SAP Security team ignores and doesn't focus on. In contrast, the Basis team limits themselves to SP upgrades that may not be happening as frequently as we would like, resulting in SAP ecosystems with known critical and High vulnerabilities, which can cause the breach.
- Work with Your Basis, SAP Security, and Cyber/Infosec teams to develop Roles and Responsibility and RACI matrix so that No team assumes the other team has it. Removing False Sense of Security.
- The Basis team is typically accountable for SAP Patch Day activities. The Basis team manages the technical aspects of the SAP system, including system administration, maintenance, and applying patches. They work closely with the Security team to apply security-related patches promptly and efficiently.

# Where to start?

To begin with SAP Patch Days, the following steps are recommended:

- Know Your Landscape. Start with Identifying various SAP Systems you, as a customer is responsible for patching Security vulnerabilities.
- Collaboration: Establish clear communication and collaboration between the Basis and Security teams.
- Schedule: Set a regular schedule for SAP Patch Days to ensure consistency and predictability.
- Risk Assessment: Conduct a risk assessment to identify the criticality of vulnerabilities and prioritize patching accordingly.
- Patch Management Policy: Develop a comprehensive policy outlining roles, responsibilities, and procedures.
- Testing the Patch: Make sure you have a testing process and a change management process before deploying the patch in production.

# Process and sample RACI

Here's a simple process flow along with RACI (Responsible, Accountable, Consulted, Informed) for SAP Patch Days:

## 1. Identify Vulnerabilities and Patches:

- Responsible: Security Team
- Accountable: Basis Team

## 2. Prioritize Patches based on Criticality:

- Responsible: Security Team
- Accountable: Basis Team
- Consulted: Functional Teams



# Process and sample RACI

## 3. Test Patches in the Test Environment:

- Responsible: Basis Team
- Accountable: Basis Team
- Consulted: Security Team
- Informed: Functional Teams

## 4. Deploy Patches to Production:

- Responsible: Basis Team
- Accountable: Basis Team
- Consulted: Security Team
- Informed: Functional Teams

# Process and sample RACI

## 5. Post-Patch Validation and Monitoring:

- Responsible: Basis Team
- Accountable: Basis Team
- Consulted: Security Team
- Informed: Functional Teams

## 6. Documentation and Reporting:

- Responsible: Basis Team
- Accountable: Security Team

# Crawl, Walk and Run, Don't try to remediate all Vulnerabilities at Once, you Will Fail....

Before embarking on SAP Patch Days, it's essential to conduct a vulnerability assessment to understand the current security posture of your SAP systems. This assessment helps identify existing vulnerabilities and areas that require immediate attention.

It's essential to recognize that attempting to address all vulnerabilities simultaneously can be overwhelming and may lead to inadequate fixes. Prioritization is key, and critical vulnerabilities should be addressed first.

Focus on fixing Critical Vulnerabilities first: Critical vulnerabilities pose the most significant risk to the system and should be prioritized for remediation.

## On Prem Vs On Cloud(S4/Rise with SAP)

Whether you are running SAP systems on-premises or with SAP's cloud solution like "Rise with SAP," security remains a shared responsibility between the organization and SAP.

While SAP ensures the security of its infrastructure and services, the organization is responsible for securing its applications, data, and configurations.

# Consider Vulnerability Scanning tool

Consider using a reliable SAP vulnerability management tool to scan and assess SAP systems for vulnerabilities.

These tools can help identify security gaps and provide insights into the most critical areas requiring attention.

Few Examples :

1. SAP Solution Manager(System Recommendations, Free, but you must invest efforts configuring it properly).
2. SAP Enterprise Threat Detection(Paid)
3. 3<sup>rd</sup> Party – Onapsis(Paid)

# Go Beyond SAP Patch Day, Build SAP Vulnerability Management Program

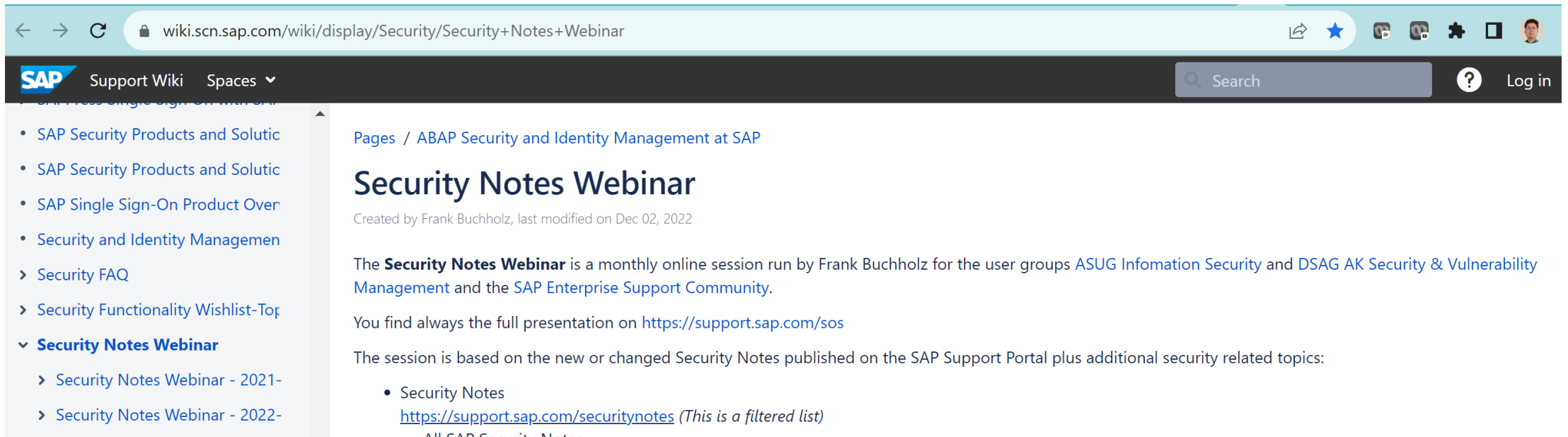
SAP Patch Days are just one aspect of a comprehensive SAP vulnerability management program. Organizations should aim to establish an ongoing process for identifying, prioritizing, and remediating vulnerabilities in SAP systems. This involves continuous monitoring, periodic risk assessments, security awareness training, and a proactive approach to security.

By following these steps and incorporating a well-defined process with the right level of accountability, organizations can enhance the security and resilience of their SAP systems while staying on top of the latest patches and updates.

# Additional Resource and tools

## ASUG Monthly Webinar

<https://wiki.scn.sap.com/wiki/display/Security/Security+Notes+Webinar>



The screenshot shows a web browser displaying the SAP Support Wiki page for the Security Notes Webinar. The browser's address bar shows the URL: [wiki.scn.sap.com/wiki/display/Security/Security+Notes+Webinar](https://wiki.scn.sap.com/wiki/display/Security/Security+Notes+Webinar). The page header includes the SAP logo, "Support Wiki", and "Spaces". A search bar and a "Log in" button are also visible. The main content area features a breadcrumb trail: "Pages / ABAP Security and Identity Management at SAP". The title "Security Notes Webinar" is prominently displayed, followed by the text "Created by Frank Buchholz, last modified on Dec 02, 2022". The body text explains that the webinar is a monthly online session run by Frank Buchholz for the user groups ASUG Information Security and DSAG AK Security & Vulnerability Management, and the SAP Enterprise Support Community. It states that the full presentation is available at <https://support.sap.com/sos>. The session is based on new or changed Security Notes published on the SAP Support Portal, plus additional security-related topics. A list of Security Notes is provided, with a link to <https://support.sap.com/securitynotes> (noted as a filtered list) and a link to "All SAP Security Notes". A left-hand navigation menu is visible, listing various topics including "SAP Security Products and Solutions", "SAP Single Sign-On Product Overview", "Security and Identity Management", "Security FAQ", "Security Functionality Wishlist-Top", and "Security Notes Webinar" (which is expanded to show "Security Notes Webinar - 2021-" and "Security Notes Webinar - 2022-").

## Additional Resource and tools

[SAP Security Optimization Services Portfolio](#)

<https://blogs.sap.com/2012/03/27/security-patch-process-faq/>

<https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html>

<https://support.sap.com/en/alm/solution-manager/processes-72/system-recommendations.html>

<https://www.sap.com/about/trust-center.html>

<https://wiki.scn.sap.com/wiki/display/Security/Security+Notes+Webinar>

<https://support.sap.com/en/offerings-programs/enterprise-support/enterprise-support-academy.html>

▪



# Questions?

For questions after this session, contact me at

<https://www.linkedin.com/in/gauravsingh14>

**Thank you.**