NCA-09.051624 – NCERT Advisory: SAP Vulnerability Alert & Security Patch Day, May 2024

Introduction

SAP, a prominent provider of enterprise software solutions, has released critical security updates as part of its May 2024 Security Patch Day. These updates address several vulnerabilities across various SAP products, including SAP NetWeaver Application Server ABAP, SAP CX Commerce, SAP Business Client, and more. Of particular concern is CVE-2024-33006, a critical vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform, which could allow attackers to achieve complete system compromise.

Impact

The vulnerabilities addressed in the security updates pose significant risks to organizations utilizing SAP products. Exploitation of these vulnerabilities could lead to various consequences, including unauthorized access, data breaches, and potential system compromise. Prompt action is essential to mitigate these risks and safeguard organizational assets.

CVE-2024-33006: Critical SAP NetWeaver Vulnerability

The most notable vulnerability addressed in the May 2024 SAP Security Patch Day is CVE-2024-33006, affecting SAP NetWeaver Application Server ABAP and ABAP Platform. This critical vulnerability, with a CVSS score of 9.6, allows unauthenticated attackers to upload malicious files to the server, potentially leading to complete system compromise upon access. SAP_BASIS versions 700 to 758 are affected by this vulnerability, necessitating immediate attention and patch application.

Other Critical Vulnerabilities

Additionally, two critical vulnerabilities, CVE-2019-17495 and CVE-2022-36364, were addressed in SAP CX Commerce, posing significant risks if left unpatched. Updates for these vulnerabilities are crucial to mitigate potential exploitation and safeguard SAP CX Commerce environments.

A ‘Hot News’ security note was issued for the Chromium browser component within SAP Business Client, underlining the importance of updating this component promptly. Furthermore, a high-priority note was released to address CVE-2024-28165, a cross-site scripting (XSS) vulnerability in the SAP BusinessObjects Business Intelligence Platform, with a CVSS score of 8.1. Organizations utilizing these components are urged to apply updates promptly to prevent potential security breaches.

Medium- and Low-Severities

Several medium- and low-severity vulnerabilities across various SAP products, including SAP S/4HANA, SAP My Travel Requests, SAP Replication Server, SAP Global Label

Management, SAP Bank Account Management, and SAP UI5, were also addressed in the latest security patches. While these vulnerabilities may have a lower impact compared to critical ones, organizations are advised to apply patches promptly to maintain the overall security posture of their SAP environments.

Recommendations & Action Items

NCERT recommends the following proactive measures to mitigate the risks associated with SAP vulnerabilities:

1. **Timely Patch Application:** Organizations should apply the latest SAP security patches promptly to address critical vulnerabilities and ensure the integrity of their systems.
2. **Conduct Vulnerability Assessments**: Perform regular vulnerability assessments and security audits to identify any weaknesses or misconfigurations in SAP systems. Address any identified issues promptly to reduce the attack surface and enhance overall security posture.
3. **Implement Least Privilege Principle**: Follow the principle of least privilege to restrict access to SAP systems only to authorized users and limit their permissions based on job roles and responsibilities. This can help prevent unauthorized access and minimize the impact of potential security breaches.
4. **Enhance Monitoring and Detection**: Implement robust monitoring and detection mechanisms to identify suspicious activities or unauthorized access attempts within SAP environments. This includes monitoring for indicators of compromise and unusual network traffic patterns.

References

1. **SAP Security Notes and News**: [https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html]
2. **SAP Security Patch Day – May 2024**: [https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2024.html]
3. **SAP Security Patching Guide**: [https://community.sap.com/t5/application-development-blog-posts/security-patch-process-faq/ba-p/12920062]

NCERT emphasizes the criticality of applying SAP security patches promptly to mitigate potential risks and ensure the continued security and integrity of organizational systems. Failure to address these vulnerabilities in a timely manner may expose organizations to significant security breaches and operational disruptions.