Critical SAP Security Notes
October Patch Day 2022

Bibin Mathew, SAP
October 20, 2022

Public

THE BEST RUN SAP

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Very High Priority Security Notes (October 2022)

Very High Priority (CVSS > 8.9) Security Notes Released

1. 3242933 - [CVE-2022-39802] File path traversal vulnerability in SAP Manufacturing Execution
2. 3239152 - [CVE-2022-41204] Account hijacking through URL Redirection vulnerability in SAP Commerce login form

We strongly advise our customers to apply these security notes immediately to protect against potential exploits and to ensure secure configuration of their SAP landscape.

3242933 - [CVE-2022-39802] File path traversal vulnerability in SAP Manufacturing Execution

- **Released on:** October 2022 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP Manufacturing Execution
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
    1. File Path Traversal– Very High
       CVSS Score: 9.9; CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- **Workaround:** Refer to solution section
- **FAQ:** Refer to solution section

3239152 - [CVE-2022-41204] Account hijacking through URL Redirection vulnerability in SAP Commerce login form

- **Released on:** October 2022 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP Commerce
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
    1. Account Hijacking– Very High
       CVSS Score: 9.6; CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- **Workaround:** Refer to solution section
- **FAQ:** 3246352

Thank you.

Contact information:

Bibin Mathew
bibin.mathew@sap.com

Follow us

www.sap.com/contactsap

THE BEST RUN SAP