Critical SAP Security Notes
May Patch Day 2024

Shrisha Banamukala, SAP
May 14, 2024

Public

Critical Security Notes (May 2024)

Critical Severity (CVSS > 8.9) Security Notes Released

1. 3455438 - [CVE-2019-17495] Multiple vulnerabilities in SAP CX Commerce
2. 3448171 - [CVE-2024-33006] File upload vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform

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.

3455438 - [CVE-2019-17495] Multiple vulnerabilities in SAP CX Commerce

- **Released on:** May 2024 Patch Day
- **Severity:** **Critical**
- **Product Affected:** SAP CX Commerce
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
    1. CSS Injection Vulnerability – Critical
       CVSS Score: 9.4; CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
    2. Remote Code Execution – Critical
       CVSS Score: 8.8; CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- **Workaround:** None

3448171 - [CVE-2024-33006] File upload vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform

- **Released on:** May 2024 Patch Day
- **Severity:** **Critical**
- **Product Affected:** SAP NetWeaver Application Server ABAP and ABAP Platform
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
    1. File upload vulnerability – Critical
       CVSS Score: 9.6; CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
- **Workaround:** Refer to Solution section

Thank you.

Contact information:

Shrisha Banamukala
Shrisha.banamukala.krishna.kumar@sap.com