Critical SAP Security Notes
July 2020 – Sep 2020

Bibin Mathew, SAP
September 29, 2020

PUBLIC

THE BEST RUN SAP

Very High Priority Security Notes (July 2020 – Sep 2020)

4 Very High Priority(CVSS > 8.9) Security Note Released

1. 2934135 - [CVE-2020-6287] Multiple Vulnerabilities in SAP NetWeaver AS JAVA (LM Configuration Wizard)
2. 2928635 - [CVE-2020-6284] Cross-Site Scripting (XSS) in SAP NetWeaver (Knowledge Management)
3. 2961991 - [CVE-2020-6320] Improper Access Control in SAP Marketing (Mobile Channel Servlet)
4. 2958563 - [CVE-2020-6318] Code Injection vulnerability in SAP NetWeaver (ABAP Server) 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.

2934135 - [CVE-2020-6287] Multiple Vulnerabilities in SAP NetWeaver AS JAVA (LM Configuration Wizard)

- **Released on:** July Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver AS JAVA (LM Configuration Wizard)
- **Impact:** Complete compromise of confidentiality, integrity and availability.
- Security Spotlight News
- **Vulnerabilities:**
    1. Missing Authentication – Very High
       CVSS Score: 10.0; CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
    2. Path Traversal - Medium
       CVSS Score: 5.3; CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
- **Workaround:** Available(refer to note's solution section)
- **FAQ:** 2948106

2928635 - [CVE-2020-6284] Cross-Site Scripting (XSS) in SAP NetWeaver (Knowledge Management)

- **Released on:** August Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver Knowledge Management
- **Impact:** Complete compromise of confidentiality, integrity and availability.
- **Vulnerabilities:**
    1. Cross-Site Scripting– Very High
       CVSS Score: 9.0; CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
- **Workaround:** Not Available
- **FAQ:** 2932212, 2957979

2961991 - [CVE-2020-6320] Improper Access Control in SAP Marketing (Mobile Channel Servlet)

- **Released on:** September Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP Marketing (Mobile Channel Servlet)
- **Impact:** Complete compromise of confidentiality and integrity
- **Vulnerabilities:**
    1. Improper Access Control – Very High
       CVSS Score: 9.6; CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
- **Workaround:** Available(refer to note's solution section)
- **FAQ:** 2963056

2958563 - [CVE-2020-6318] Code Injection vulnerability in SAP NetWeaver (ABAP Server) and ABAP Platform

- **Released on:** September Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver (ABAP Server) and ABAP Platform
- **Impact:** Complete compromise of confidentiality, integrity and availability.
- **Vulnerabilities:**
    1. Code Injection vulnerability – Very High
       CVSS Score: 9.1; CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
- **Workaround:** Not Available
- **FAQ:** 2965897

Thank you.

Contact information:

Bibin Mathew
SAP Security Response
bibin.mathew@sap.com

THE BEST RUN SAP®