Security Advisory 2021-020

SAP - Critical Vulnerabilities

April 15, 2021 — v1.0

TLP:WHITE

Summary

On the 13th of April 2021, SAP released 14 Security Notes on the Security Patch Day [1]. Security Note #3040210 [2] addresses a critical vulnerability CVE-2021-27602 [3] affecting the SAP Commerce. Another critical vulnerability CVE-2021-21481 [4] in Security note #3022422 [5] is affecting the MigrationService, which is part of SAP NetWeaver.

Security Note #2622660 [6] refers to a vulnerability that impacts SAP Business Client, a user interface that acts as an entry point to various SAP business applications. The security risk resides not in the product itself, but in the browser control (Chromium) that comes with it. There are no details about the issue, except that it has been rated with a the maximum severity score, **10 out of 10**.

Technical Details

The vulnerability CVE-2020-27602 has **CVSS score 9.9** [3]. SAP Commerce, versions - 1808, 1811, 1905, 2005, 2011, back-office application allows certain authorised users to create source rules which are translated to drools rule when published to certain modules within the application. An attacker with this authorisation can inject malicious code in the source rules and perform remote code execution enabling them to compromise the confidentiality, integrity and availability of the application.

The vulnerability CVE-2021-21481 has **CVSS score 9.6** [4]. The MigrationService, which is part of SAP NetWeaver versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform an authorisation check. This might allow an unauthorised attacker to access configuration objects, including such that grant administrative privileges. This could result in complete compromise of system confidentiality, integrity, and availability.

Products Affected

- SAP Commerce, Versions - 1808, 1811, 1905, 2005, 2011
- SAP NetWeaver versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50

Recommendations

Considering the seriousness of the flaw, and the fact that **exploits are already available**, CERT-EU strongly advises to **apply available patches as soon as possible**.

References

[1] https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649

[2] https://launchpad.support.sap.com/#/notes/3040210

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27602

[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21481

[5] https://launchpad.support.sap.com/#/notes/3022422

[6] https://launchpad.support.sap.com/#/notes/2622660