Security Advisory 2021-026

SAP - Critical Vulnerabilities

June 9, 2021 — v1.0

TLP:WHITE

History:

- *9/06/2021 — v1.0 – Initial publication*

Summary

On 8th of June 2021, SAP released 17 Security Notes. There were two updates to previously released Patch Day Security Notes [1].

Among the vulnerabilities there are two rated critical, with a CVSS above 9:

- **CVE-2021-27602** - Remote Code Execution vulnerability in Source Rules of SAP Commerce
- **CVE-2021-27610** - Improper Authentication in SAP NetWeaver ABAP Server and ABAP Platform

Technical Details

Security Note #3040210 [2] addresses a critical vulnerability CVE-2021-27602 [3] affecting SAP Commerce. This is an update of a previous published vunerability we have aslo adressed in our advisory [6].

The vulnerability CVE-2020-27602 has **CVSS score 9.9**. 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 [3].

Security Note #3007182 [5] addresses a critical vulnerability CVE-2021-27610 [4] affecting SAP NetWeaver AS ABAP and ABAP Platforms.

The vulnerability CVE-2021-27610 has **CVSS score 9** [4]. This vulnerability is an improper authentication in SAP NetWeaver ABAP Server and ABAP Platform.

Products Affected

- SAP Commerce, Versions - 1808, 1811, 1905, 2005, 2011
- SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 804

Recommendations

Considering the seriousness of the flaws CERT-EU strongly advises to **apply available patches as soon as possible**.

References

[1] https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999

[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-2021-27610

[5] https://launchpad.support.sap.com/#/notes/3007182

[6] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-020.pdf