CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-034

SAP - Critical Vulnerability

July 16, 2020 — v1.1

TLP:WHITE

History:

- *14/07/2020 — v1.0 – Initial publication*
- *16/07/2020 — v1.1 – Update with information on exploits available*

Summary

On the 14th of July 2020, SAP released eight Security Notes on the Security Patch Day [1]. Security Note `#2934135` [2] addresses a critical vulnerability CVE-2020-6286 [3] affecting the SAP NetWeaver Application Server (AS) Java component LM Configuration Wizard. Through a vulnerability dubbed RECON by Onapsis who discovered the flaw [9], an unauthenticated attacker take control of trusted SAP applications. As of 16th of July 2020, exploits have been released and active scanning for the vulnerability is ongoing [8].

Technical Details

The vulnerability CVE-2020-6286 has **CVSS score 10** [3]. SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check [3].

According to Onapsis, this is a very serious vulnerability affecting a default component present in every SAP application running the SAP NetWeaver Java technology stack. This technical component is used in many SAP business solutions, SAP S/4HANA Java, SAP SCM, SAP CRM, SAP Enterprise Portal, SAP Solution Manager (SolMan) and many others [9].

If the vulnerability is successfully exploited, a remote and unauthenticated attacker can obtain unrestricted access to SAP systems through the creation of high-privileged users. The execution of arbitrary operating system commands with the privileges of the SAP service user account (`<sid>adm`) which is a user at the operating system level [6], has unrestricted access to the SAP database and is able to perform application maintenance activities [7].

Exploits are already publicly available, and active scanning for this vulnerability has been observed.

Products Affected

This vulnerability is present by default in SAP applications running on top of SAP NetWeaver AS Java Versions - 7.30, 7.31, 7.40, 7.50. Potentially vulnerable SAP business solutions include any SAP Java-based solutions such as:

- SAP Enterprise Resource Planning,
- SAP Product Lifecycle Management,
- SAP Customer Relationship Management,
- SAP Supply Chain Management,
- SAP Supplier Relationship Management,
- SAP NetWeaver Business Warehouse,
- SAP Business Intelligence,
- SAP NetWeaver Mobile Infrastructure,
- SAP Enterprise Portal,
- SAP Process Orchestration/Process Integration),
- SAP Solution Manager,
- SAP NetWeaver Development Infrastructure,
- SAP Central Process Scheduling,
- SAP NetWeaver Composition Environment, and
- SAP Landscape Manager.

Recommendations

Considering the seriousness of the flaw, and the fact that exploits are already available, **CERT-EU strongly advises to apply available patches [6] as soon as possible**.

References

[1] https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675

[2] https://launchpad.support.sap.com/#/notes/2934135

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6287

[4] https://launchpad.support.sap.com/#/notes/2939665

[5] https://us-cert.cisa.gov/ncas/alerts/aa20-195a

[6] https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.00/en-US/be98c998bb5710149e8cace9b0
html

[7] https://launchpad.support.sap.com/

[8] https://www.bleepingcomputer.com/news/security/poc-exploits-released-for-sap-recon-vulnerabilities-patch-now/

[9] https://www.onapsis.com/recon-sap-cyber-security-vulnerability