CERT-EU

Security Advisory 2022-011

ICM Vulnerability in SAP Software

February 9, 2022 — v1.0

TLP:WHITE

History:

- *09/02/2022 — v1.0 – Initial publication*

Summary

On February 8, the SAP Product Security Response Team released new patches addressing CVEs in SAP products [1]. One of them is categorised as critical vulnerabilitY with the CVSS score of 10. This vulnerability identified as `CVE-2022-22536` is affecting many SAP products and it can lead to different impacts such as: ransomware attack, theft of sensitive data, financial fraud, disruption of mission-critical business processes, etc.

No proof-of-concept or ongoing exploitation of these vulnerabilities have been observed yet. However, it is highly recommended to apply the patch as soon as possible.

Technical Details

The vulnerability `CVE-2022-22536` is particularly critical because this issue is present by default in the ICM component. ICM is the SAP component that enables HTTP(S) communications in SAP systems. Since ICM is exposed to the internet and untrusted networks by design, vulnerabilities in this component have an increased level of risk.

The attack, known as HTTP request smuggling, could be used to steal credentials and session information from unpatched SAP servers, even if servers are placed behind proxies. According to Onapsis: *"A simple HTTP request, indistinguishable from any other valid message and without any kind of authentication, is enough for a successful exploitation."* [2].

Affected Products

- SAP Web Dispatcher, versions: 7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87,
- SAP Content Server, version: 7.53,
- SAP NetWeaver and ABAP Platform, versions: KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49.

Recommendations

SAP Product Security Response Team recommends to apply the Security Updates detailed in [1].

References

[1] https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022

[2] https://therecord.media/cisa-and-sap-warn-about-major-vulnerability/