Security Advisory 2021-004

Critical Vulnerability in SAP Solution Manager

January 22, 2021 — v1.0

TLP:WHITE

History:
- 22/01/2021 — v1.0 – Initial publication

Summary

On the 10th of March 2020, SAP released several patches for their products. One of them fixes a critical vulnerability in SAP Solution Manager - User-Experience Monitoring. This vulnerability could lead to remote code execution on every system connected to the Solution Manager [1]. Last week, a proof-of-concept has been publicly released [2], thus increasing the compromise possibility. Applying the patch is highly recommended.

Technical Details

Identified by CVE-2020-6207, this vulnerability is due to missing authentication checks. A remote, unauthenticated attacker could exploit this weakness to deploy and execute scripts and operating system commands on all SMDAgents connected to the Solution Manager [3].

Affected products

The following product is affected by the vulnerability:
- SAP Solution Manager 7.2

Recommendations

It is recommended to apply the patches from SAP for all servers.
References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6207
