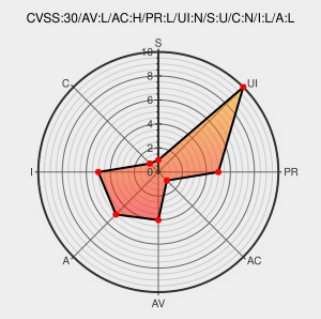
CVE-2021-21470

Published on: 01/12/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:58 PM UTC

CVE-2021-21470

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Enterprise Performance Management from Sap contain the following vulnerability:

SAP EPM Add-in for Microsoft Office, version - 1010 and SAP EPM Add-in for SAP Analysis Office, version - 2.8, allows an authenticated attacker with user privileges to parse malicious XML files which could result in XXE-based attacks in applications that accept attacker-controlled XML configuration files. This occurs as logging service does not disable XML external entities when parsing configuration files and a successful exploit would result in limited impact on integrity and availability of the application.

CVE-2021-21470 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP EPM Add-in for Microsoft Office** version **1010**

Affected Vendor/Software: **SAP SE** - **SAP EPM Add-in for SAP Analysis Office** version **2.8**

CVSS3 Score: 4.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	LOW

CVSS2 Score: 3.6 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SAP Security Patch Day – January 2021 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476
No Description Provided	Permissions Required launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/3000291

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Enterprise Performance Management	1010	All	All	All
Application	Sap	Enterprise Performance Management	2.8	All	All	All
Application	Sap	Enterprise Performance Management	1010	All	All	All
Application	Sap	Enterprise Performance Management	2.8	All	All	All

cpe:2.3:a:sap:enterprise_performance_management:1010:*:*:*:*:microsoft_office:*:*:

cpe:2.3:a:sap:enterprise_performance_management:2.8:*:*:*:*:sap_analysis_office:*:*:

cpe:2.3:a:sap:enterprise_performance_management:1010:*:*:*:*:microsoft_office:*:*:

cpe:2.3:a:sap:enterprise_performance_management:2.8:*:*:*:*:sap_analysis_office:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→