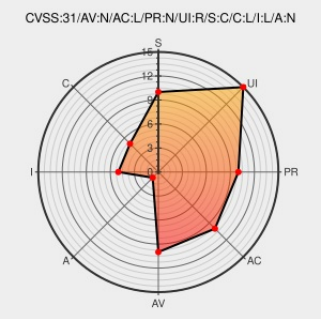
CVE-2018-17861

Published on: 08/09/2021 12:00:00 AM UTC

Last Modified on: 08/13/2021 07:22:00 PM UTC

CVE-2018-17861

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



Certain versions of J2ee Engine from Sap contain the following vulnerability:

** UNSUPPORTED WHEN ASSIGNED ** A cross-site scripting (XSS) vulnerability in SAP J2EE Engine/7.01/Portal/EPP allows remote attackers to inject arbitrary web script via the wsdlLib parameter to /ctcprotocol/Protocol. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2018-17861 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Bugtraq: SAP J2EE Engine/7.01/Portal/EPP Reflected Cross Site Scripting (XSS)	seclists.org text/html	BUGTRAQ 20190304 SAP J2EE Engine/7.01/Portal/EPP Reflected Cross Site Scripting (XSS)

Full Disclosure: SAP J2EE Engine/7.01/Portal/EPP Reflected Cross Site Scripting (XSS)	seclists.org text/html	FULLDISC 20190305 SAP J2EE Engine/7.01/Portal/EPP Reflected Cross Site Scripting (XSS)
SAP J2EE Engine/7.01/Portal/EPP Protocol Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/151945/SAP-J2EE-Engine-7.01-Portal-EPP-Protocol-Cross-Site-Scripting.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	J2ee Engine	7.01	All	All	All

cpe:2.3:a:sap:j2ee_engine:7.01:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→