ESUP-2022-AVI-001 - CVE-2022-22965

Utilisation et diffusion de ce document

Les avis de sécurité du consortium ESUP-Portail portent sur des vulnérabilités des logiciels diffusés par le consortium. Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit, pour des raisons évidentes de sécurité des Systèmes d'Information de tous les établissements du consortium ESUP-Portail.

Objet	CVE-2022-22965 vis à vis des applications ESUP
Référence	ESUP-2022-AVI-001
Date de la première version	1 avril 2022
Date de la dernière version	11 avril 2022
Source	CVE-2022-22965
Diffusion de cette version	Publique
Historique	• 31 mars 2022 : réception de la faille https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement (Pascal Rigaux) • 31 mars 2022 : reproduction de l'exploit via des POC (Pascal Rigaux, David Lemaignent, Valentin Hagnéré, Vincent Bonamy) • 31 mars 2022 : reproduction de l'exploit sur esup-dematec (Vincent Bonamy) • 1 avril 2022 : envoi d'un mail à esupdematec-devel@esup-portail.org • 1 avril 2022 : rédaction de l'avis (Coordination Technique) • 1 avril 2022 : envoi de l'avis de sécurité à securite@esup-portail.org • 11 avril 2022 : modification de l'avis pour indiquer qu'il reste préférable de disposer de briques à jour • 11 avril 2022 : envoi de l'avis de sécurité à esup-utilisateurs@esup-portail.org
Planning prévisionnel	-
Pièces jointes	-

Risque

- Possibilité pour un attaquant d'envoyer et faire exécuter du code arbitraire à un serveur.

Systèmes affectés

- Cette vulnérabilité peut impacter les applications spring déployées en jdk 9 ou supérieur, notamment avec un Tomcat (externe)
- la version 5.3.18 de spring a pour objet de combler la faille.

Description

Suivant l'implémentation des applications et la possibilité pour un anonyme notamment d'effectuer des "POST", cette vulnérabilité est plus ou moins exploitable.

L'exploitation de la faille telle que proposée dans les scripts POC consiste à :

- identifier une url (avec mappage d'objet) comme vulnérable
- envoyer des paramètres pouvant provoquer l'écriture sur le serveur d'application d'un fichier
- ce fichier peut correspondre à une jsp qui peut permettre d'exécuter un code arbitraire sur le serveur.

Solutions

Plusieurs solutions sont disponibles.

- le mieux est de mettre à jour les librairies spring et donc les applications proposant ces mises à jour
- on peut aussi repasser sur l'usage d'un openjdk 8 puisque seules les versions supérieures permettent l'exploit
- on peut aussi mettre à jour Tomcat (8.5.78 ou 9.0.62 ou 10.0.20 qui ferment la vulnérabilité connue).

Applications concernées

EsupDematEC 1.9.0 déployée sur un Tomcat avec un jdk11
EsupDematEC 1.9.1 (et supérieur) embarque les librairies spring à jour

Applications potentiellement concernées

Potentiellement les applications utilisant certaines fonctionnalités de spring-webmvc et déployées sur un Tomcat avec un jdk9 ou supérieur.

Ainsi des nouvelles versions sont proposées pour Apereo CAS et Shibboleth IdP.

Pour les applications ESUP, de nouvelles versions sont également disponibles pour esup-sgc, esup-nfc-tag, esup-emargement, esup-papercut, esup-pay, esup-signature, ecandidat, esup-mdw (Esup MonDossierWeb), ...

Applications non concernées

- bbb : à priori pas vulnérable et utilise un tomcat embedded
- esup-smsu : utilise spring-webmvc mais utilise @RequestBody qui ne semble pas être affecté par la faille
- ecandidat, fwa, esup-mdw : référencent spring-webmvc mais ne l'utilisent que pour proposer des méthodes/controller sans mapping d'objet ; ne proposant donc pas d'url permettant d'exploiter la faille
- grouper, pstage : n'utilisent pas spring-webmvc
- EsupUserApps, ProlongationENT, Ametys, Nuxeo : n'utilisent pas Spring
- ... et toutes les applications non java

Dans tous les cas, il est préférable de disposer de briques à jour, notamment vis-à-vis de cette faille :

- *des serveurs d'application tomcat à jour (fermant la vulnérabilité connue)*
- *des applications proposant des librairies spring à jour (fermant la vulnérabilité connue)*

Liens

- Blog Spring.io du 31 mars 2022 https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- CVE-2022-22965 de VMware https://tanzu.vmware.com/security/cve-2022-22965
- CVE-2022-22965 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
- CERTFR-2021-ALE-022 : https://www.cert.ssi.gouv.fr/avis/CERTFR-2022-AVI-297/