Novembre 2021



Nouveautés de la version 3.20.1



# Préambule

Les SDIS concernés par les anomalies contenant le mot clé « Oracle » sont, par ordre alphabétique : le SDIS 68, le SDIS 78 et le SDMIS (SDIS 69). Ces SDIS ne sont pas concernés par les anomalies contenant le mot clé « MySQL » ou « MariaDB ».

Les autres SDIS ne sont pas concernés par les anomalies « Oracle » mais sont concernés par les anomalies contenant le mot clé « MySQL ».

Les SDIS concernés par les anomalies « GPEC » sont, par ordre alphabétique : le SDIS 44, le SDIS 59 et le SDIS 86. Les autres SDIS ne sont pas concernés par les anomalies « GPEC ».

# Général

## CG01 : Renfort de protection contre une vulnérabilité potentielle XSS impliquant l'utilisation d'un courriel de phishing sur un utilisateur déjà connecté à l'applicatif et l'usage d'un serveur tiers pouvant permettre, dans de rares cas, d'exfiltrer l'identifiant de session temporaire d'un utilisateur

Un lien envoyé dans un courriel et pointant vers une page spécifique pouvait permettre d’afficher une image en erreur avec l’exécution d’un Javascript au niveau du poste client pouvant permettre avec une certaine difficulté d’obtenir le cookie de session de l’utilisateur et de l’exfiltrer vers un site tiers. Cette vulnérabilité a été détectée et protégée, elle n’a pas été mise en œuvre à notre connaissance.

Les conditions nécessaires pour sa mise en œuvre :

1. L’acteur malveillant doit avoir :
	1. Les connaissances requises en sécurité informatique ;
	2. Un serveur externe accessible par le poste de l’utilisateur cible ;
	3. La connaissance de cette vulnérabilité – donc un accès préalable à GEEF ;
	4. La connaissance du nom du cookie de session GEEF – qui change à chaque redémarrage de l’applicatif ;
	5. La connaissance du nom de l’utilisateur cible et de ses accès ;
	6. Envoyer un mail à l’utilisateur cible contenant le lien ;
2. L’utilisateur cible doit :
	1. Avoir un accès intéressant pour l’acteur malveillant (administrateur, de préférence) ;
	2. Recevoir le mail sans que celui-ci n’ait été filtré par un filtre antispam ou anti-phishing ;
	3. Être connecté à GEEF avant de…
	4. … cliquer sur le lien
3. GEEF doit être :
	1. Accessible à l’utilisateur cible et à l’acteur malveillant (accès externe à priori) ;
	2. En version antérieure à cette version ;
	3. Ne pas être protégé par un reverse proxy qui filtre les adresses contenant du code HTML ou Javascript.

Nous publierons des détails sur la mise en œuvre aux clients intéressés lorsque tous les autres clients auront passé une version supérieure ou égale à celle-ci.

# Formation

## EF01 : Modification de la feuille de présence modèle "68" pour prise en compte des périodes d'animations multiples sur une même journée



Ces modèles ont été revus pour regrouper les périodes d’animations des formateurs.

## CF01 : Correction d'une anomalie potentielle lorsque tous les services sont décochés pour l'enregistrement de l'écran "Formation / Administration > FMPA > FMPA par service"CG01 : …



Lorsque des services étaient cochés dans cet écran, il n’était plus possible de décocher tous les services, un message d’erreur apparaissait à la place et la modification n’était pas prise en compte.