

Sécurité applicative : l'industrie manufacturière à l'épreuve

Veracode, éditeur de solutions de tests de sécurité des applications, a livré le volet industriel de son rapport 2021 sur l'état de la sécurité logicielle (SOSS)*.

Que retenir de cette édition sectorielle de [l'étude](#) ?

L'industrie manufacturière se situe dans la moyenne lorsque l'on considère le taux d'applications utilisées contenant au moins une faille de sécurité (76% tout de même).

La proportion de failles critiques est même inférieure à la moyenne dans la production (21%, contre 24% tous secteurs confondus).

En revanche, cette industrie tarde plus que d'autres à réagir.

297 jours pour colmater les brèches

Les entreprises de ce secteur affichent ainsi le taux le plus faible de correction de vulnérabilités (59% des failles sont corrigées).

Les failles les plus souvent repérées dans l'industrie sont les suivantes :

1. Fuite de données
2. Faille CRLF (Carriage Return Line Feed)
3. Défaut de qualité du code
4. Problème de chiffrement
5. Défaut de gestion des informations d'identification

Or, les acteurs de l'industrie manufacturière mettent davantage de temps à colmater les brèches (durée médiane de 297 jours).

Alors que, globalement, le délai médian de correction des vulnérabilités, d'une faille CRLF au défaut de qualité du code, est de 86 jours après leur découverte.

Le fournisseur américain de solutions fait le constat suivant : l'industrie peut mieux faire.

« Avec les cycles lents que l'on retrouve dans de nombreux systèmes de [contrôle industriel](#) et embarqués, ces résultats ne sont pas inattendus, mais ils restent décevants. »

* Veracode « The State of Software Security v11 – Industry Snapshot: Manufacturing »*