



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Atlassian
Numéro de Référence	47592305/24
Date de Publication	23 Mai 2024
Risque	Critique
Impact	Critique

Systemes affectés

- Jira Software Server versions antérieures à 9.4.20
- Jira Software Server versions antérieures à 9.15.2
- Jira Software Server versions antérieures à 9.12.7
- Jira Software Data Center versions antérieures à 9.8.0
- Jira Software Data Center versions antérieures à 9.7.2
- Jira Software Data Center versions antérieures à 9.4.20
- Jira Software Data Center versions antérieures à 9.15.2
- Jira Software Data Center versions antérieures à 9.12.7
- Jira Software Data Center versions antérieures à 9.12.0
- Jira Software Data Center versions antérieures à 9.11.3
- Confluence Data Center versions antérieures à 8.9.1
- Confluence Data Center versions antérieures à 8.5.9
- Confluence Data Center versions antérieures à 7.19.22

Identificateurs externes

- CVE-2022-25647 CVE-2022-41966 CVE-2023-45859 CVE-2024-1597 CVE-2024-21683 CVE-2024-22257 CVE-2024-23672 CVE-2024-24549

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits Atlassian susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service, de porter atteinte à la confidentialité des données et d'exécuter du code arbitraire à distance.

Solution :

Veillez se référer au bulletin de sécurité Atlassian du 23 Mai 2024 pour plus d'information.

Risque :

- Exécution du code arbitraire à distance
- Déni de service
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité Atlassian du 23 Mai 2024:

- <https://confluence.atlassian.com/security/security-bulletin-may-21-2024-1387867145.html>