Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 20 juin 2022
N° CERTFR-2022-AVI-570

Affaire suivie par: CERT-FR

AVIS DU CERT-FR

Objet: Multiples vulnérabilités dans les produits IBM

Gestion du document

Référence	CERTFR-2022-AVI-570
Titre	Multiples vulnérabilités dans les produits IBM
Date de la première version	20 juin 2022
Date de la dernière version	20 juin 2022
Source(s)	Bulletin de sécurité IBM 6596145 du 17 juin 2022 Bulletin de sécurité IBM 6596155 du 17 juin 2022 Bulletin de sécurité IBM 6572497 du 17 juin 2022 Bulletin de sécurité IBM 6596085 du 17 juin 2022
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Risque(s)

- Exécution de code arbitraire à distance
- Déni de service à distance
- Contournement de la politique de sécurité
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données

Systèmes affectés

- IBM StoredIQ versions 7.6.0.x antérieures à 7.6.0.22 sans le correctif de sécurité siq_7_6_0_22_log4j_2_17_1
- IBM Security Guardium versions 10.5 sans le correctif de sécurité SqlGuard_10.0p550_Bundle_Mar-27-2022
- IBM Security Guardium versions 10.6 sans le correctif de sécurité SqlGuard_10.0p692_Bundle_May-12-2022
- IBM Security Guardium versions 11.0 sans le correctif de sécurité SqlGuard_11.0p45_Bundle_May-03-2022
- IBM Security Guardium versions 11.1 sans le correctif de sécurité SqlGuard_11.0p160_Bundle_Mar-23-2022
- IBM Security Guardium versions 11.2 sans le correctif de sécurité SqlGuard_11.0p270_Bundle_Feb-24-2022
- IBM Security Guardium versions 11.3 sans le correctif de sécurité SqlGuard_11.0p360_Bundle_Mar-24-2022
- IBM QRadar WinCollect Agent versions 10.0.x antérieures à 10.0.2

Résumé

De multiples vulnérabilités ont été découvertes dans les produits IBM. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité.

Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

Documentation

- Bulletin de sécurité IBM 6596145 du 17 juin 2022
  https://www.ibm.com/support/pages/node/6596145
- Bulletin de sécurité IBM 6596155 du 17 juin 2022
  https://www.ibm.com/support/pages/node/6596155
- Bulletin de sécurité IBM 6572497 du 17 juin 2022
  https://www.ibm.com/support/pages/node/6572497
- Bulletin de sécurité IBM 6596085 du 17 juin 2022
  https://www.ibm.com/support/pages/node/6596085
- Référence CVE CVE-2021-44228
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
- Référence CVE CVE-2021-45046
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
- Référence CVE CVE-2021-45105
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
- Référence CVE CVE-2016-5397
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5397
- Référence CVE CVE-2018-11798
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11798
- Référence CVE CVE-2018-1320
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1320
- Référence CVE CVE-2019-0205
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0205
- Référence CVE CVE-2019-0210
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0210

- Référence CVE CVE-2020-13949
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13949
- Référence CVE CVE-2022-1434
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1434
- Référence CVE CVE-2022-1343
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1343
- Référence CVE CVE-2022-1292
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1292
- Référence CVE CVE-2022-1473
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1473
- Référence CVE CVE-2021-22947
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22947
- Référence CVE CVE-2022-22576
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22576
- Référence CVE CVE-2021-22945
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22945
- Référence CVE CVE-2022-27774
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27774
- Référence CVE CVE-2022-0778
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
- Référence CVE CVE-2022-27776
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27776
- Référence CVE CVE-2021-22946
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22946
- Référence CVE CVE-2022-27775
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27775
- Référence CVE CVE-2021-3712
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3712

Gestion détaillée du document

le 20 juin 2022
Version initiale
