

BULLETIN D'ALERTE

N°0125-BA001


 Bonne Année
 à toutes nos parties
 Prenantes

Multiplés Vulnérabilités dans les produits Apache

Origine : GN-CERT/ANSSI
 Date de l'alerte : 02/01/2025

ABSTRACT

Le 02 Janvier 2025, le GN-CERT a observé des vulnérabilités dans Apache Hive, Apache Spark, Apache Hadoop, Apache Mina et Apache Traffic Control. Plates-formes largement utilisées pour le traitement, l'analyse de ... à grande échelle...

Ces vulnérabilités pourront être exploitées pour obtenir un accès non autorisé aux systèmes touchés et bien plus...

Ce bulletin d'actualité présente les informations dont le **GN-CERT** a connaissance à ce jour concernant ces vulnérabilités.

DESCRIPTIONS

1. VULNERABILITE DANS APACHE HIVE ET APACHE SPARK

Le composant de service Apache Hive expose accidentellement le cookie signé à l'utilisateur final lorsqu'il y a une incompatibilité de signature entre le cookie actuel et le cookie attendu. L'exposition de la signature de cookie correcte peut entraîner une exploitation ultérieure.

La logique vulnérable CookieSigner a été introduite dans Apache Hive par HIVE-9710 (1.2.0) et dans Apache Spark par SPARK-14987 (2.0.0).

Les composants concernés sont les suivants

- org.apache.hive:service-ruche
 - org.apache.spark:spark-hive-thriftserver_2.11
 - org.apache.spark:spark-hive-thriftserver_2.12
- **CVE-2024-23945** : Apache Hive, Apache Spark (CookieSigner expose la signature correcte lorsque la vérification du message échoue)
 - **CWE-367** : Génération d'un message d'erreur contenant des informations sensibles
 - **Gravité** : Score CVSSv3.x **5.9 MOYEN, Urgent.**
 - **Métrique** : CVSS :3.1/AV :N/AC :H/PR :N/UI :N/S :U/C :N/I :H/A :N
 - **Score d'exploitabilité** : 2.2
 - **Score d'impact** : 3.6

2. VULNERABILITE CRITIQUE D'INJECTION SQL DANS APACHE TRAFFIC CONTROL

Une vulnérabilité critique dans Apache Traffic Control une Plate-forme open source largement utilisée pour la création de réseaux de diffusion de contenu (CDN) à grande échelle. La vulnérabilité pourrait être exploitée pour exécuter du code malveillant sur les systèmes affectés.

Les composants concernés sont les suivants

Apache Traffic Control 8.0.0 à 8.0.1

Versions Corrigées

Apache Traffic Control version 8.0.2 ou plus

- **CVE-2024-45387** : Apache Traffic Control (Injection SQL dans le point de terminaison Traffic Ops PUT deliveryservice_request_comments)
- **CWE-89 : Neutralisation incorrecte d'éléments spéciaux dans une commande SQL**
- **Gravité** : Score CVSSv3.x **9.9 CRITIQUE, Très Urgent.**
- **Métrique** : CVSS :3.1/AV :N/AC :L/PR :L/UI :N/S :C/C :H/I :H/A :H
- **Score d'exploitabilité** : 3.1
- **Score d'impact** :

3. VULNERABILITE CRITIQUE D'EXECUTION DE CODE A DISTANCE DANS APACHE MINA

La vulnérabilité existe dans le composant ObjectSerializationDecoder, qui manque de contrôles de sécurité lors du traitement des données sérialisées. Les attaquants peuvent exploiter cela en envoyant des données sérialisées malveillantes spécialement conçues, pouvant conduire à l'exécution de code à distance (RCE).

Les composants concernés sont les suivants

- Apache MINA 2.0 à 2.0.26
- Apache MINA 2.1 à 2.1.9
- Apache MINA 2.2 à 2.2.3
- **CVE-2024-52046** : Apache MINA (Les applications MINA utilisant la désérialisation illimitée peuvent autoriser RCE)
- **CWE-94 : Contrôle inapproprié de la génération de code (injection de code)**
- **Gravité** : Score CVSSv3.x **10.0 CRITIQUE, Très Urgent.**
- **Métrique** : CVSS :4.0/AV : N/AC :L/AT :N/PR :N/UI :N/VC :H/VI :H/V...

4. VULNERABILITE DE CONTOURNEMENT DE L'AUTHENTIFICATION DANS APACHE HUGEGRAPH-SERVER

Une vulnérabilité critique de contournement de l'authentification a été découvert dans Apache HugeGraph-Server, une base de données de graphes open source largement utilisée.

Les composants concernés sont les suivants

- Apache HugeGraph-Server 1.0 à 1.3
- **CVE-2024-4344** : Apache HugeGraph-Server (Jeton JWT fixe)
- **CWE-302** : Contournement de l'authentification par des données supposées immuables
- **Versions Corrigées**
 - ✓ Apache HugeGraph-Server 1.5.0

SYSTEMES AFFECTÉS

Les vulnérabilités affectent les produits suivants

1. Vulnérabilité dans Apache hive et apache spark

- Apache Hive 1.2.0 à 4.0.0
- Apache Spark 2.0.0 à 3.0.0
- Apache Spark 3.0.0 à 3.3.4
- Apache Spark 3.4.0 à 3.4.2
- Apache Spark 3.5.

2. Vulnérabilité critique d'injection sql dans apache traffic control

- Apache MINA 2.0 à 2.0.26
- Apache MINA 2.1 à 2.1.9
- Apache MINA 2.2 à 2.2.3

3. Vulnérabilité critique d'exécution de code à distance dans apache mina

- Apache MINA 2.0 à 2.0.26
- Apache MINA 2.1 à 2.1.9
- Apache MINA 2.2 à 2.2.3

4. Vulnérabilité de contournement de l'authentification dans apache hugegraph-server

- Apache HugeGraph-Server 1.0 à 1.3



MESURES À PRENDRE

Le **GN-CERT** recommande les mesures suivantes :

1. Pour apache hive et apache spark

- À titre de mesure temporaire, envisagez de mettre en place des contrôles de validation supplémentaires sur les signatures de cookies avant de les traiter. Cela peut aider à atténuer le risque d'exploitation jusqu'à ce que les packages puissent être mis à jour. Par exemple, vous pouvez ajouter une couche middleware qui vérifie l'intégrité des cookies avant qu'ils ne soient utilisés dans votre application.
- Mettre à jour les paquets concernés vers leurs versions corrigées.
Pour Apache Hive, effectuez une mise à niveau vers la version 4.0.0 ou ultérieure. Pour Apache Spark, mettez à jour vers la version 3.4.2 pour le package spark-hive-thriftserver_2.12 et assurez-vous que le package spark-hive-thriftserver_2.11 est mis à jour vers une version ultérieure à la version 2.4.8.

2. Pour l'injection sql dans apache traffic control

Mettre à jour vers les versions corrigées suivantes

- Apache Traffic Control version 8.0.2 ou plus

3. Pour l'exécution de code à distance dans apache mina

Mettre à jour vers les versions corrigées suivantes

- Apache MINA 2.0.27
- Apache MINA 2.1.10
- Apache MINA 2.2.4

Après la mise à niveau, définissez explicitement les classes autorisées pour la désérialisation à l'aide de l'un des nouveaux suivants

- `accept(ClassNameMatcher classNameMatcher)`
- `accept(Pattern pattern)`
- `accept(String... patterns)`

4. Pour le contournement de l'authentification dans apache hugegraph-server

Mettre à jour vers les versions corrigées est **Apache HugeGraph-Server 1.5.0**

Veillez diffuser ces informations à vos filiales et partenaires et partager avec nous toute information et constatation pertinente.

Le GN-CERT reste à votre disposition pour toute information supplémentaire ou assistance à la correction de ces vulnérabilités ou encore tout service de conseil et réponses aux incidents.

REFERENCES

- <https://nvd.nist.gov/vuln/detail/CVE-2024-23945>
- <https://lists.apache.org/thread/5o2ljinzrv8zvhjw9vy7b4rwjpc32hgfc>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-45387>
- <https://lists.apache.org/thread/h2607yv32wgcrywov960jpxhvsmlf12>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-52046>

AUTRES LIENS POUR RESTER INFORME

- <https://www.facebook.com/ANSSIGN>
- <https://twitter.com/AnssiGuinee>