NVD DB Update

CVE-2023-25194 - Score: 8.8

Components:

apache kafka connect *

Description:

A possible security vulnerability has been identified in Apache Kafka Connect API. This requires access to a Kafka Connect worker, and the ability to create/modify connectors on it with an arbitrary Kafka client SASL JAAS config and a SASL-based security protocol, which has been possible on Kafka Connect clusters since Apache Kafka Connect 2.3.0. When configuring the connector via the Kafka Connect REST API, an authenticated operator can set the ‘sasl.jaas.config‘ property for any of the connector’s Kafka clients to "com.sun.security.auth.module.JndiLoginModule", which can be done via the ‘producer.override.sasl.jaas.config‘, ‘consumer.override.sasl.jaas.config‘, or ‘admin.override.sasl.jaas.config‘ properties. This will allow the server to connect to the attacker’s LDAP server and deserialize the LDAP response, which the attacker can use to execute java deserialization gadget chains on the Kafka connect server. Attacker can cause unrestricted deserialization of untrusted data (or) RCE vulnerability when there are gadgets in the classpath. Since Apache Kafka 3.0.0, users are allowed to specify these properties in connector configurations for Kafka Connect clusters running with out-of-the-box configurations. Before Apache Kafka 3.0.0, users may not specify these properties unless the Kafka Connect cluster has been reconfigured with a connector client override policy that permits them. Since Apache Kafka 3.4.0, we have added a system property ("-Dorg.apache.kafka.disallowed.login.modules") to disable the problematic login modules usage in SASL JAAS configuration. Also by default "com.sun.security.auth.module.JndiLoginModule" is disabled in Apache Kafka Connect 3.4.0. We advise the Kafka Connect users to validate connector configurations and only allow trusted JNDI configurations. Also examine connector dependencies for vulnerable versions and

https://cybersword.tech
www.linkedin.com/in/cybersword-tech
ph1sher
@davidwowa