Severity

High

Analysis Summary

CVE-2022-24706, CVSS: 9.8

Apache CouchDB could allow a remote attacker to gain elevated privileges on the system, caused by improper access control to an improperly secured default installation. By sending a specially-crafted request, an attacker could exploit this vulnerability to gain admin privileges to execute arbitrary code on the system.

CVE-2022-23942, CVSS: 7.5

Apache Doris could allow a remote attacker to obtain sensitive information, caused by the use of a hardcoded key and IV to initialize the cipher used for ldap password. By utilize cryptographic attack techniques, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

Impact

- Gain Privileges
- Code Execution
- Information Theft

Indicators Of Compromise

CVE

- CVE-2022-24706
- CVE-2022-23942

Affected Vendors

- Apache

Affected Products

- Apache CouchDB 3.2.1
- Apache Doris 0.15.0

Remediation

Refer to Apache Security Advisory for the patch, upgrade, or suggested workaround information.

CVE-2022-24706

CVE-2022-23942