Severity

High

Analysis Summary

CVE-2022-29266

Apache could allow a remote attacker to obtain sensitive information, caused by an error logic in the dependency library lua-resty-jwt that leak secrets in error response. By sending a specially-crafted JSON Web Token to a route protected by the jwt-auth plugin, an attacker could exploit this vulnerability to obtain the plugin-configured secret information, and use this information to launch further attacks against the affected system.

Impact

Information Disclosure

Indicators Of Compromise

CVE

CVE-2022-29266

Affected Vendors

Apache

Affected Products

- Apache APISIX 2.13.0

Remediation

Upgrade to the latest version of Apache APISIX, available from the Apache Web site.

Apache Web site