

Organizations Warned of Security Risk in Default Apache Superset Configurations

Malicious attackers can exploit Apache Superset installations running default configurations to gain administrator access and execute code on servers and databases, penetration testing firm Horizon3.ai warns.

An open source application written in Python and based on the Flask web framework, Apache Superset provides users with the ability to explore and visualize large amounts of data.

The same as other Flask-based applications, Superset uses session cookies that are signed with a secret key for authentication.

The secret key is supposed to be randomly generated, to prevent scenarios where an attacker could use a known key to sign their own cookies and gain access to the application.

An attacker who knows a Superset session key could log in as an administrator, access databases connected to the application, add, modify or delete databases, and execute code remotely, both on databases and on the server.

“By default, database connections are set up with read-only permissions but an attacker with admin access can enable writes and DML (data model language) statements. The powerful SQL Lab interface allows attackers to run arbitrary SQL statements against connected databases,” Horizon3.ai explains.

Furthermore, the attacker could harvest sensitive information, including user password hashes and database credentials in plaintext.

Tacked as CVE-2023-27524 (CVSS score of 8.9), the vulnerability identified by Horizon3.ai exists because, when Superset is installed, the secret key is defaulted to a specific value, with the user being responsible for changing it to a cryptographically secure random string.

The security firm initially discovered and reported the bug in October 2021. The secret key value was rotated in January 2022 to a new default and a warning was added to the logs.

In February 2023, Horizon3.ai discovered that there were over 3,000 Superset instances accessible from the internet, and that more than 2,000 of them (roughly two thirds) were using a default secret key. Apache Superset versions up to 2.0.1 are impacted.

“Among the 2000+ affected users, we found a broad mix of large corporations, small companies, government agencies, and universities. We sent out good-faith notifications to a number of organizations, some of whom remediated shortly after,” the company notes.

The vulnerability was addressed in Superset version 2.1, which prevents the server from starting if a default secret key is in use. Superset instances that are installed via a docker-compose file or a helm template, however, still use default keys.

Other Flask-based applications were also found vulnerable to the hardcoded secret key bug, including Apache Airflow (CVE-2020-17526) and Redash (CVE-2021-41192).

Related: Critical Apache Commons Text Flaw Compared to Log4Shell, But Not as Widespread

Related:High-Severity Vulnerability Found in Apache Database System Used by Major Firms

Related:High-Risk Flaw Haunts Apache Server

Organizations Warned of Security Risk in Default Apache Superset Configurations