Partek Flow Security

Log4j Vulnerability

Partek Flow follows a two-week patch cycle to address any Critical rated vulnerabilities located in any Partek Flow components. Partek Flow does not make use of Log4j components and is not vulnerable to CVE-2021-44228.

Data Access Controls

Partek Flow software resists external or internal compromise via isolation between users, groups, and data. This isolation is tunable by the Partek Flow administrator as well as users that need to increase the visibility of the data they own. Collections of per-account roles and permissions allow the administrator to define coarse or fine-grain data access rules. Once the administrator configures user privacy directories, users cannot see one another's data on the same Partek Flow server unless they are collaborators on the same project.

Authentication

Accounts are protected by a username and password authentication over HTTPS. Authentication credentials are protected using industry-standard approaches like salting, password complexity checks, and administrator-controlled account lockouts. To conform with existing corporate security standards, administrators can use LDAP instead of the Partek Flow internal authentication.

Data Transit Security

All data uploaded and downloaded through Partek Flow is transited using HTTPS. Keys are provided by the Partek Flow administrator, and thus can be as secure as policy dictates.

Auditing

All user and administrator actions are immutably logged and timestamped.

Application Security

All Partek Flow components are kept up to date. Should a security vulnerability be identified it will be immediately rectified. The Partek Flow server and its sub-processes are run with limited privileges, thus damage from a compromised Partek Flow server is minimized. Third-party user-added executable files are restricted from running unless contained within a dedicated folder. Partek Flow is compatible with additional containment strategies such as Docker or virtualization.

Infrastructure Security

Given the minimal deployment requirements of Partek Flow, it is easily integrated into existing infrastructure. The design of this surrounding infrastructure can significantly increase or weaken the security of a Partek Flow deployment. The Partek operations and development team has experience deploying Partek Flow in a variety of environments including cloud, cluster, and desktop, each with varying security requirements. We are available to assist administrators with recommendations on infrastructure design, deployment, and backup.

Data Integrity and Reproducibility

All parameters and steps taken to generate results using Partek Flow are tracked and easily allow for the reproduction of past results or detailed auditing. Partek Flow detects and reports external modification of user data. Partek performs internal tests to ensure data generated by Partek Flow is scientifically accurate and consistent with previous results.

Additional Assistance

If you need additional assistance, please visit our support page to submit a help ticket or find phone numbers for regional support.

Your Rating:

Results: 34 rates