Outage and Upgrade Communication

TDS maintenance windows are scheduled every Wednesday 5-7 PM CET. Operations team deploys service upgrades, patches, or changes. Most deployments are implemented within 15 minutes, however more complex changes can take 30 minutes or longer. Users are informed about all planned changes in advance, longer outages are highlighted in the communication.

Planned Changes

Planned changes deliver regular service upgrades and infrastructure changes.

Service	Communication Channel and Timeframe
Jira and Confluence	Application banner - 48h in advance
Artifactory, Bitbucket, Gitlab, Subversion, SeedDMS	Application banner - 48h in advance (not available for SeedDMS and Subversion) E-mail - 5 calendar days in advance, addressed to TDS project owners and SaaS project/space /repository admins (Users for Subversion)*****
Dedicated SaaS (SaaS applications dedicated to one or multiple TDS projects)	SPOC and named stakeholders are informed by agreed channels 5 calendar days in advance Application banner 48 hours prior to the change (if requested by SPOC)
TDS Portal	TDS portal is upgraded frequently through the automated continuous delivery pipeline with a few seconds of downtime in most cases. Since this is not a business-critical application and upgrades are performed very frequently, users are not informed about outages. New functionality is described in Release Notes.

*) Deployed during 2022-10 – respective toolkit needs to be implemented to generate list or e-mail recipients

Regular schedule of maintenance windows can be occasionally altered (e.g. longer outages are scheduled for the weekend instead of Wednesday evening).

Emergency Changes

Emergency changes (typically high or critical security patches) are deployed as soon as possible. Users are informed through the same communication channels as for planned changes, but the time between user communication and change deployment is shorter. Note that critical security vulnerabilities are often patched within 24 hours after CVE is published.

Servers

Virtual servers are dedicated to TDS projects and project teams are responsible for performing regular server maintenance. In case of critical security vulnerabilities, the TDS operations team patches these servers with high priority as soon as possible. Automatic security updates are enabled by default on CentOS and Ubuntu servers, hence intervention from TDS operations team should be exceptional. Server admins (and named SPOC if applicable) are informed in advance as soon as possible via e-mail or chat.

CVE's

To check current CVE mitigation rules please navigate to CVE Mitigations

Related Pages

Release Notes | Service description (Including Service Level Agreement) | Service Status | Roadmap