Incident regarding the availability of the backend CA services

Started	18.03.2024 15:12
Closed	18.03.2024 15.58
Services affected	Backend CA services and issuance and usage of disposable certificates
Description	At approximately 15:12, users began reporting sluggish performance and inability to access certain functionalities within the third-party application integrated with the backend CA services and in particular for the issuance and usage of disposable certificates. Few minutes earlier our monitoring systems detected a spike in connection requests to the database server, the incident response team was immediately notified, and investigation procedures were initiated to identify the underlying cause. Logs from both the applications and the backend services were analyzed to pinpoint the source of the issue. Unfortunately, the sudden surge in connections quickly led to the exhaustion of available resources on the database server, resulting in delays in query execution and eventual timeouts for third party applications.
Root cause	Further investigation revealed that recent updates to one of the components of the CA backend inadvertently introduced a flaw in connection management. As a result, the application was establishing and holding onto a larger number of database connections than necessary, exacerbating the issue of connection saturation. To alleviate the immediate impact of the incident, the database connection pool settings were adjusted to allow for a higher number of concurrent connections temporarily. Additionally, the

	affected applications were restarted to clear any lingering connections and restore normal functionality.
Personal data impacted (privacy)	No impacts
Remediation action	A permanent fix is under development to address the underlying issue with connection management in the application code. This fix involved optimizing connection handling and implementing connection pooling mechanisms to prevent future instances of connection saturation. Further next steps include also: 1. Conduct a post-incident review to analyze the effectiveness of the response and identify areas for improvement. 2. Review existing monitoring and alerting systems to ensure early detection of similar issues in the future. 3. Provide additional training to development teams on best practices for connection management and database optimization.