

# Incident Report 110315

---

On March 15, 2011, the Projectplace online service was affected by a Denial of Service incident that led to a global service outage. The following report describes the details of the incident, its effect on the service, and how the issue was resolved.

## Summary

At 14.20, the number of application processes on the Projectplace frontend servers rose quickly and unexpectedly. Server resources such as processor power got consumed rapidly, which resulted in the Projectplace online service becoming unresponsive and eventually completely unavailable to its users. All frontends were so severely affected by the incident that they had to be taken offline.

The assessment of the situation was finished at 14.55, and system recovery was initiated. Due to minor issues, this process was delayed by a couple of minutes. A partial recovery was reached at 15.06 when Projectplace started accepting new incoming requests. The service reached full recovery at 15.34 when all frontends were fully available again.

The Projectplace web site was available the whole time, but it was not possible to log into or work with the service. During the course of the outage, no data was lost.

## Additional Details

We could establish the root cause of the incident through log analysis and system forensics. An architectural weakness in the event handling for the database objects can expose a Denial of Service vulnerability to the Projectplace web application. In order to exploit the vulnerability, a set of circumstances for an object has to be met.

## Improvement Actions

Projectplace takes system outages very seriously. Our commitment is demonstrated in our drive to build redundancy and resilience into everything that we develop. Despite this commitment, though, things can always go wrong.

We are sorry that this outage caused our customers trouble and inconvenience. Please rest assured that we monitor our systems 24 x 7, we have engineers available to analyze and resolve production issues 24 x 7, we are staffed to respond quickly to problems, and we develop ongoing improvements to our systems to proactively make them better and to prevent recurrence of problems.

A post-mortem database analysis showed that the probability of a future incident with a similar cause is very low. However, due to the potential impact of the issue, we have revised the risk assessment for this type of weakness and taken appropriate mitigation actions. They include hard- and software upgrades for our application frontends, as well as a revision of the system architecture for object and event handling.

The incident also revealed weaknesses in our incident management process that need to be addressed. Operations Management has taken measures in order to improve our incident response and speed up system recovery if a similar issue was to occur in the future.

## Version History

Version Number	Date	Author	Change Comment
1.0	2011-03-16	WW	Initial version