DEON PMP – Patch Management Policy

Update Policy Overview

DEON provides regular updates of the offered software products. These contain both bug fixes and feature enhancements.
Usually these updates are first published in the cloud or distributed to the cloud users after comprehensive internal automated and manual tests (in the case of client software also by external beta testers).
Afterwards the updates will be distributed to OnPrem customers. This ensures that only verified stable versions are used in OnPrem environments, as hotfixes and bug fixes can be provided much more quickly in the cloud.

Vulnerability levels

DEON divides vulnerabilities into three categories:

1. Security vulnerability
2. Critical application error
3. Application error

Patching procedures

1. As soon as a security vulnerability or a critical application error becomes known, it is analysed immediately and with the highest priority internally.
   This usually happens within 12 hours of becoming known.
2. Afterwards, customers are informed about the effects of the error and recommendations for action are issued.
   At the same time, an estimate is made of the effort required to correct the error.
   Customers are informed about the expected availability of the update.
3. Once the update is available, it will be distributed to all customers.

3rd-category application error patches are distributed as part of regular application updates. Usually, client software updates occur every 3 months. Updates to the server software are provided semi-annually if necessary.