# 2020.05 Security Incident Status


- Helvetios Cluster
- Fidis Cluster
- Deneb Cluster
- All clusters
    - SSH Host Keys change
    - User SSH keys


## Helvetios Cluster

- All administration and compute nodes have been reinstalled with the latest version of RHEL 7.6
- The software stack has not changed

## Fidis Cluster

- All administration and compute nodes have been reinstalled with the latest version of RHEL 7.6
- The software stack has not changed
- (2020-06-11) Shifter is again available on the Fidis cluster (access to the image gateway from the other clusters is not yet possible)
- Some parts of the service are not yet restored, we are working on these and will bring them back as soon as possible
    - Data transfer node: fdata1.epfl.ch

## Deneb Cluster

- The administration nodes have been reinstalled with RH 7.6, the login and compute nodes will remain on RH 7.4 for compatibility with the currently available software stack/environment.
    - `deneb1.epfl.ch` (2020-06-08), `deneb2.epfl.ch`, and the **GPU partition** are now available (2020-06-04).
    - The rest of the nodes will NOT be restored as Deneb has reached its End of Life already.
- For access to your data while the cluster is unavailable Deneb's `/scratch` can be accessed on the Fidis login node, `fidis.epfl.ch` , under `/deneb_scratch` .

## All clusters

### SSH Host Keys change

Be aware that you will see a warning upon logging into the clusters:

```
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
```

This is normal as the ssh host keys changed, please see the following webpage for the current keys: Connecting to the clusters

### User SSH keys

We have deleted all users `.ssh` as a precaution measure.

The attacks reported on other HPC sites seem to have been using compromised user SSH keys.

Knowing that:

- some users have accounts in multiple sites
- it is likely that the same key is used for multiple sites
- once a key is compromised, any private keys stored in an account to which that key has access must also be considered compromised (in particular if they have no password set)

Since it is impossible to get a full list of keys that might have been compromised at other sites, and to check which other accounts and (potentially) keys those compromised keys might have given access to, we chose to err on the side of caution and remove all private and public keys from all accounts.

We understand this might be cumbersome but it is the only way to ensure that any eventual unauthorized access has been closed.