A Race for Security: Identifying Vulnerabilities on 50 000 Hosts Faster than Attackers

When operating a large scale grid infrastructure, it is important to manage a number of security risks that could impact its availability. A general security rule states that any infrastructure is as weak as its weakest link and therefore, it is essential to ensure that all resources in the infrastructure offer a similar level of security. However, the experience gathered over several years of operations in the EU EGEE / EGI infrastructures clearly shows that ensuring a homogeneous level of security across multiple, often heterogeneous, resources is challenging. This is especially the case for applying software security updates, which can require service downtime, sufficient technical expertise and a sufficient degree of coordination. Unfortunately, failure to promptly apply security updates remains one of the main causes of security incidents affecting computing infrastructures, as we can conclude from the incidents observed in the Grid environment. In this contribution, we will present the open-source service Pakiti that makes it possible to monitor patches across a large number of machines and provide a current overview about their patching status. Using Pakiti, a system operator can detect a machine where the patching process failed for whatever reason or has not been triggered at all. Pakiti offers a central view of the patching status of the infrastructure it monitors, based on packages installed and on information about known vulnerabilities. The results are displayed to the operators in a coherent manner. For example, it is possible to centrally display the exact list of hosts vulnerable to a particular vulnerability. After several years of development, Pakiti has become a robust and scalable service capable of handling thousands machines. We will describe the architecture of Pakiti and basic scenarios that can be addressed using Pakiti. Pakiti is also a key service used by the EGI security operations to monitor the whole infrastructure of EGI. We will present details about the utilization of Pakiti in EGI and other large-scale infrastructures and demonstrate how Pakiti has contributed to higher level of security of these environments.

Primary authors : PROCHAZKA, Michal (CESNET) ; KOURIL, Daniel (CESNET) ; WARTEL, Romain (CERN) ; KANELLOPOULOS,