Hello,

well, yes, as all Containers are running under one kernel on a Hardware Node, if someone trigger a kernel panic, all the Containers on this node will be affected. This is a "minus".

* but in fact not all exploits will work inside a Container, and this is a "plus".
* next thing - not in all cases you'll have to wait for a manual reboot:

  - first and the most useful in the current situation: you can add "panic=N" kernel option to the bootloader config and the kernel will reboot the node automatically after "N" seconds after it got a panic. This option really works in the 99% cases when you get an oops.
  - second: you can ask D.C to configure remote power control - simplest PDU or more intelligent separate card inserted to the server if possible - quite a widespread feature nowadays.

BTW, can you please share your experience - how many oopses due to exploits have you got for some period of time? (+ how many nodes there were total and how often did you upgrade kernels on them).

Thank you!

--
Konstantin