Subject: CVE-2016-7910 CVE-2016-7911
Posted by wyckaoo on Thu, 24 Nov 2016 09:07:12 GMT
View Forum Message <> Reply to Message

hi, CVE-2016-7910 and CVE-2016-7911 vulnerabilities are related to block devices.
As simsfs is layer between node block device and container. Does it theoretically allow to escape containers that are using simfs?

Subject: Re: CVE-2016-7910 CVE-2016-7911
Posted by vaverin on Thu, 24 Nov 2016 09:58:50 GMT
View Forum Message <> Reply to Message

CVE-2016-7910 and CVE-2016-7911 are fixed because they are marked as critical in Google security bulletin.
We do not understand how it's possible to use it for "execute arbitrary code within the context of the kernel."

Yes, theoretically it can allow an escape container,
and yes, I think simfs-based containers can be affected too.
However I doubt that someone outside Google understand how to exploit it in real life.
I even not sure that Google knows it, probably it is just an theoretical possibility.

However we think it can be used to crash host from inside container,
and it was enough for us to close this issue.

There are no according bugs in Red Hat bugzilla.
There are bugs in Novell bugzilla, but its severity is quite low, they also do not see how it can be use for the "gain privileges".

Thank you,
Vasily Averin