When American tech journalists see the words "vulnerability" and "Huawei" in close proximity these days, they tend to get over-excited and, as a result, produce copy that goes quite wonky.

A classic example of this was seen this week when the site, ZDNet, one of the tech powerhouses, reported on a patch submitted to the Linux kernel project by someone who called Huawei Kernel Self Protection.

The patch was found to have some trivial flaws by the maker of the Grsecurity kernel patch, Brad Spengler ? a man who loves publicity and knows that picking a hole in a patch put out by someone who was seemingly associated with Huawei would generate interest among the US press.

He was right. But it's a pity that ZDNet did not take some time to check its facts, with its security writer Catalin Cimpanu theorising that this patch had "sparked interest in the Linux community as (sic) could signal Huawei's wish to possibly contribute to the official kernel".

Cimpanu has a history of screwing up when it comes to Linux. Huawei has been a contributor to the Linux kernel for quite a few years now. As one commenter on the US news aggregation site Slashdot pointed out, in 2017, Huawei was 15th in the list for top companies contributing to the Linux kernel, 4.8? 4.13, and third (after Intel and Google) in in the
list of companies bringing in the most new developers.

Again, there are numerous people in numerous companies who make contributions to the Linux kernel on their own time; all patches are scrutinised by Linux creator Linus Torvalds, or one of his trusted lieutenants, before they are finally merged.

Hence, the excitement over some flaws in a patch is not really understandable.

[2]

Security

Source URL: http://www.tuxmachines.org/node/137603

Links: