Richard Hughes: Breaking apart Dell UEFI Firmware CapsuleUpdate packages

By *Roy Schestowitz*
Created *02/06/2019 - 2:33pm*
Submitted by Roy Schestowitz on Sunday 2nd of June 2019 02:33:12 PM Filed under Red Hat [1] Hardware [2] GNOME [3]

When firmware is uploaded to the LVFS we perform online checks on it. For example, one of the tests is looking for known badness like embedded UTF-8/UTF-16 BEGIN RSA PRIVATE KEY strings. As part of this we use CHIPSEC (in the form of chipsec_util -n uefi decode) which searches the binary for a UEFI volume header which is a simple string of _FVH and then decompresses the volumes which we then read back as component shards. This works well on plain EDK2 firmware, and the packages uploaded by Lenovo and HP which use IBVs of AMI and Phoenix. The nice side effect is that we can show the user what binaries have changed, as the vendor might have accidentally forgotten to mention something in the release notes.

[4]

Red Hat Hardware GNOME

Links:
[1] http://www.tuxmachines.org/taxonomy/term/142
[2] http://www.tuxmachines.org/taxonomy/term/39

[3] http://www.tuxmachines.org/taxonomy/term/146
[4] https://blogs.gnome.org/hughsie/2019/06/02/breaking-apart-dell-uefi-firmware-capsuleupdate-packages/