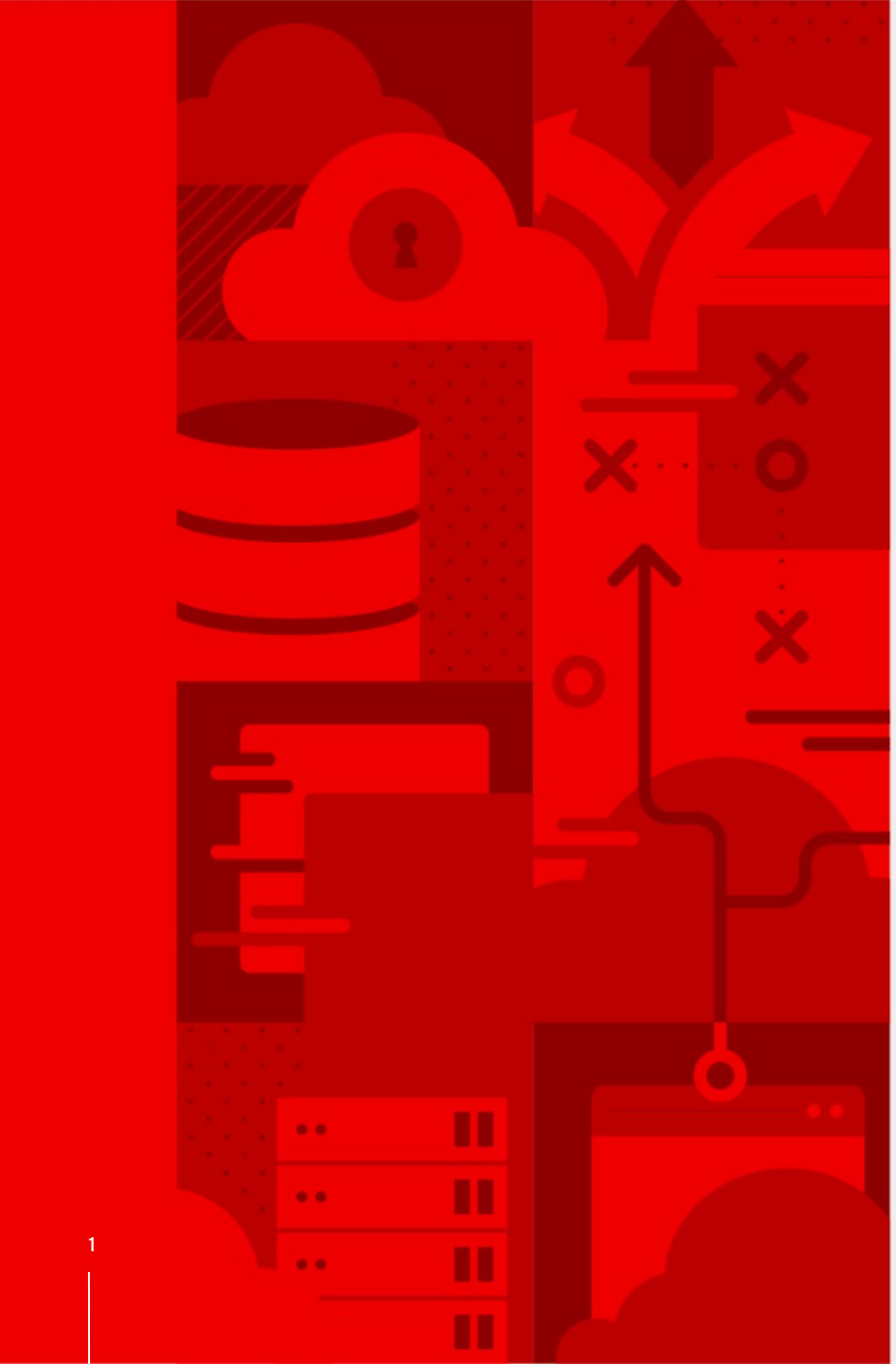


LVFS:
CERT Vendor Meeting

An overview of the ecosystem, showing some of the cool new things we're trying to do.

Richard Hughes
Principal Engineer

Red Hat

Who am I?

Building Open Source

for **over 15 years.**

Firmware troublemaker

for **7 years.**

Red Hat

LVFS and fwupd work together

LVFS : Trusted Metadata Source

The hardware vendor uploads firmware to the LVFS where it is verified and signed. Users then download a shared metadata catalogue from a central server.

fwupd : Mechanism

The open source fwupd project deploys the update onto the Linux client machine. Over 35 update protocols are now supported and more are planned.

LVFS : Anonymous Reporting

After updating firmware, fwupd optionally sends success or failure information back to the LVFS to ensure updates are being deployed without problems

The LVFS grows every year, as new vendors join and as more firmware is uploaded

Companies and agencies are free to mirror the LVFS for privacy or scalability reasons and so we don't actually know the real number of downloads.

53.2M

Firmware files supplied to end users

Since the LVFS started the official server has supplied millions of firmware updates for over 200 different devices.

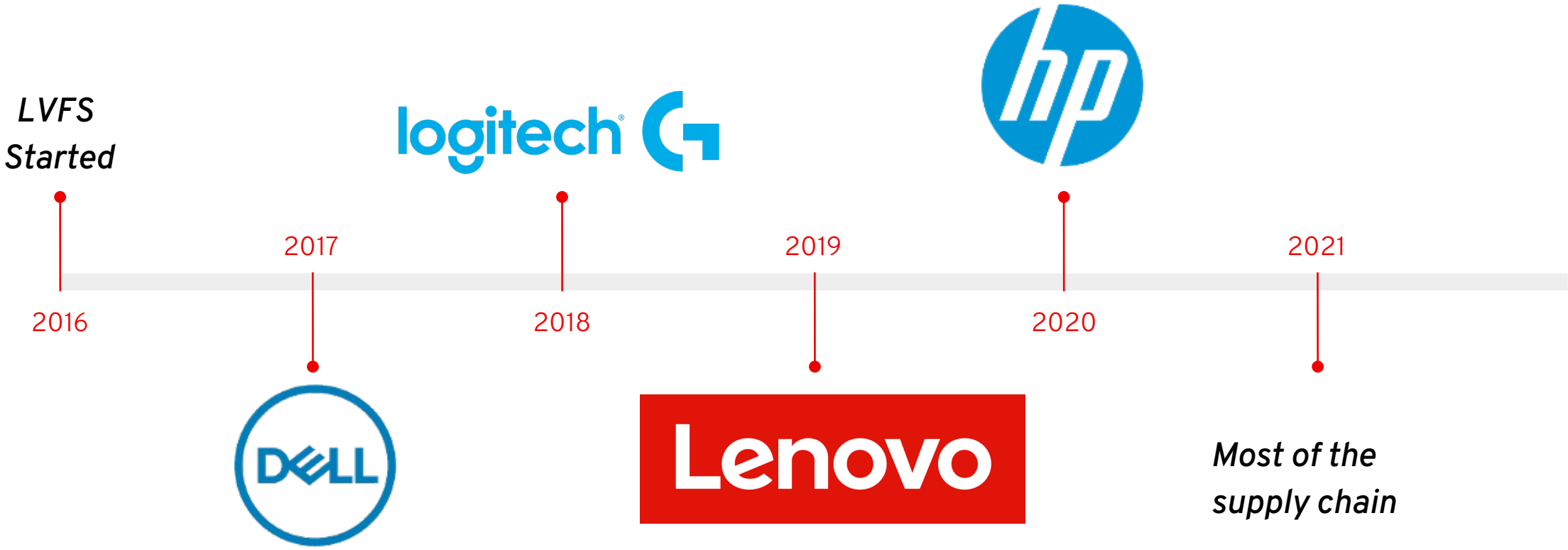
126K

Success reports from end users

Over 99% of firmware was deployed correctly, with 1% of "known failures" identified using a built-in rule engine.

Red Hat

Over 150 OEMs, ODMs and IHVs use the LVFS



Red Hat

It’s actually hard to not support the LVFS.

OEMs are free to choose whatever criteria they like for hardware suppliers, and they are choosing these rules for various business reasons.

Lenovo

All suppliers for Lenovo ThinkPad, ThinkStation and ThinkCentre have to have working fwupd plugins and be able to upload to the LVFS. Failure to meet either criteria causes the “preferred vendor” status to be lost.

Dell

All approved ODMs and ISVs being used by Dell must have firmware that can be updated using fwupd and have updates available on the LVFS.

Google

Firmware must be updatable using fwupd to get the “Designed for Chrome” compliance sticker. Google are shipping parts of fwupd in nearly every Chromebook now sold.

What the vendors are saying...

> LVFS is strategically important for Dell to be able to provide secure firmware updates in a standards-compliant way.

Mario Limonciello
Sr. Principal Software Engineer, Dell

> Standardizing on LVFS has helped Lenovo seamlessly distribute our firmware updates to our customers

Rob Herman
Executive Director, Lenovo

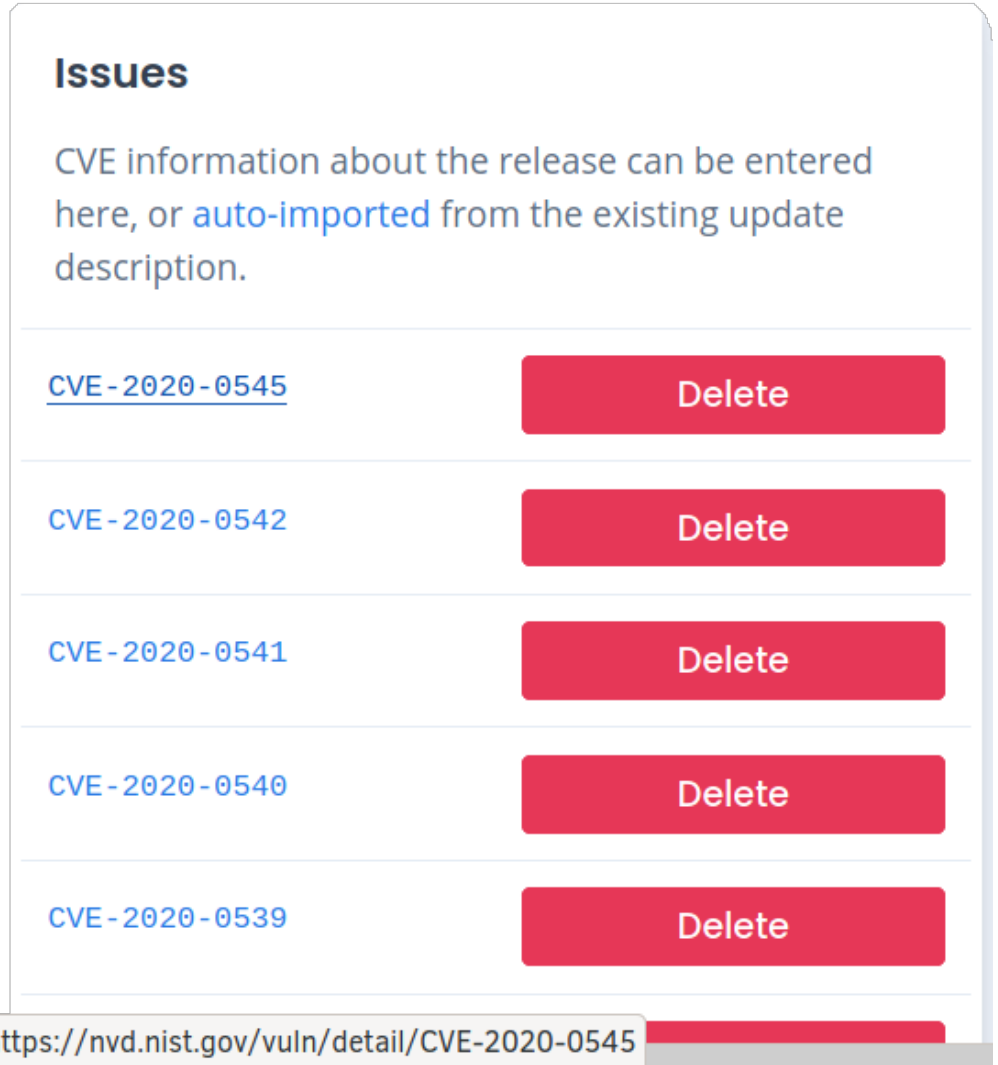
Red Hat

There is no cost to use the LVFS or to contribute to fwupd

The Linux Vendor Firmware Service is sponsored by the Linux Foundation and most development work is provided by Red Hat.

Independent consulting companies provide technical help and training.

Tying the ecosystem together



Red Hat

Firmware Analysis : Raising the Bar

Blocklist

Use a simple blocklist to check firmware for problems

Enabled

Values

DO NOT TRUST::IBV example certificate being used
DO NOT SHIP::IBV example certificate being used
To Be Defined By O.E.M::IBV example DMI data being used
c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192::Contains the Dual EC backdoor for the NSA
Do not trust::IBV example certificate being used

Modify

Red Hat

Using FwHunt we remind vendors about the embargo

```
hex_strings:
  - 56e8.........593c01....80be....000000
    # 56                                    push    esi
    # E8 .. .. .. ..                       call    x_BiosSsaEnabled
    # 59                                    pop     ecx
    # 3C 01                                 cmp     al, 1
    # .. ..                                 jnz     short loc_FFDE86FD
    # 80 BE .. .. 00 00 00                  cmp     byte ptr [esi+81h], 0
    # .. ..                                 jz      short loc_FFDE86FD
  - 6a006a0268be00000056e8
    # 6A 00                                 push    0
    # 6A 02                                 push    2
    # 68 BE 00 00 00                        push    0BEh
    # 56                                    push    esi
    # E8 .. .. .. ..                       call    SsaApi
```

LVFS end-to-end with uSWID export

coreboot — vf490ec2adc210907e3f27599c2c6fed2f1505e63 `a9032c9d-2aaa-5a25-a0e6-6d865b24e6d2`

Summary	coreboot is a project to develop open source boot firmware for various architectures	
Product	coreboot	
Colloquial Version	63c440f4e9a2466dd4a6f8c750621341a2c5ec79	
Entity	9elements	TAG_CREATOR SOFTWARE_CREATOR
Generator	uSWID	

Intel-Microcode — v2021-04-28 `cc85d5d6-357c-59f8-beb4-f0ff66965f16`

Summary	Micrcode Updates for Intel Processors	
Product	Intel-Microcode	
Entity	9elements	TAG_CREATOR
Generator	uSWID	

Red Hat

Vendors take a long time to roll out fixes