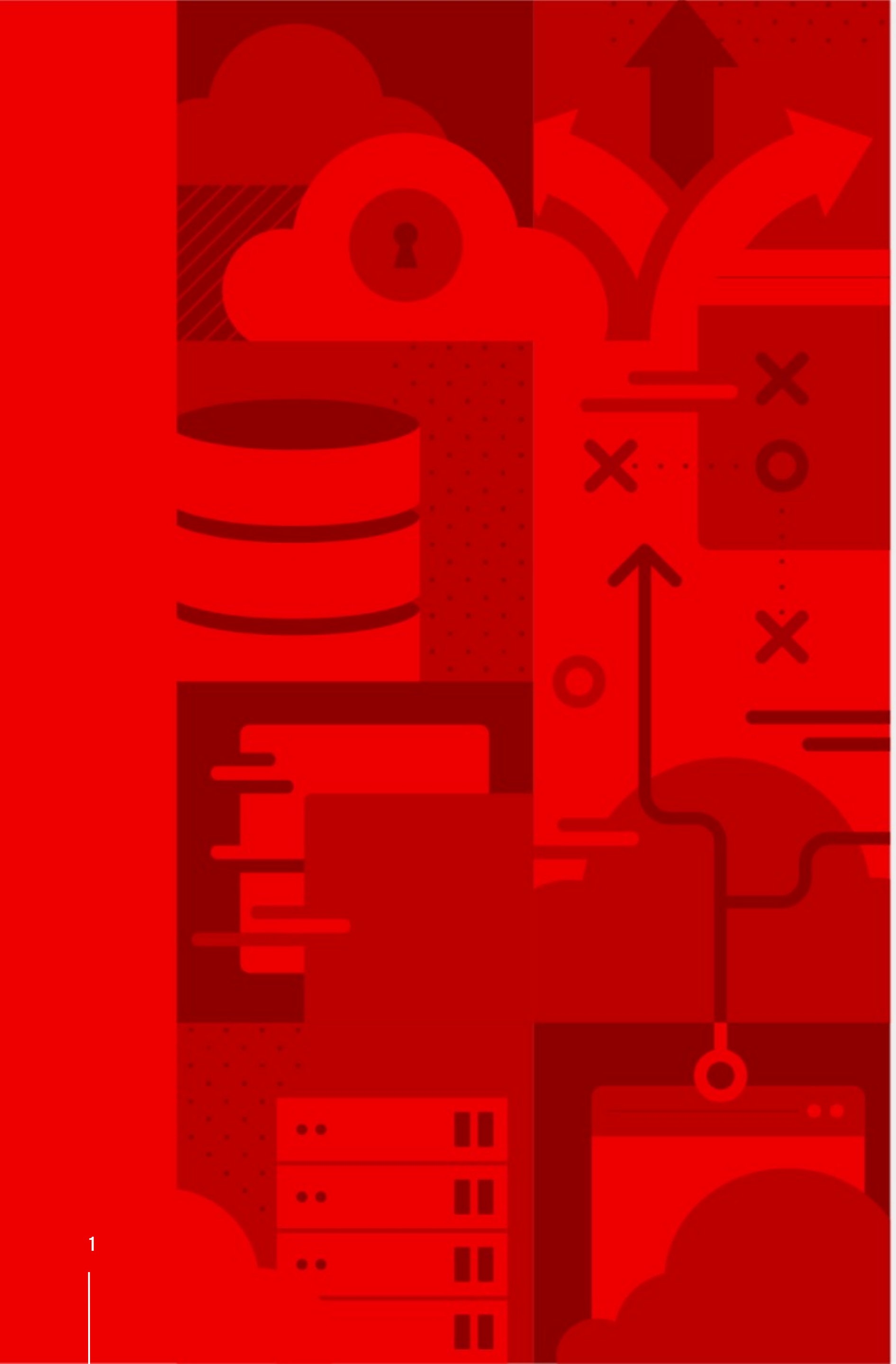


Introduction to LVFS

An overview of the ecosystem for SCITT, showing some of the implausible things we’re trying to do.

Richard Hughes
Senior Principal Software Engineer

Red Hat

Who am I?

Building Open Source

for **over 15 years.**

A *firmware troublemaker*

for over 7 years.

Users were not updating firmware

What hardware is installed?

Users don't typically know exactly what hardware they are using.

What updates are available?

Users do not visit OEM websites to manually look for firmware updates.

Are the firwmare binaries safe?

Many OEMs have insecure download links without any file checksums or signatures.

How to apply the update?

Vendor tools often required Microsoft Windows, or unsupported Linux versions.

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.

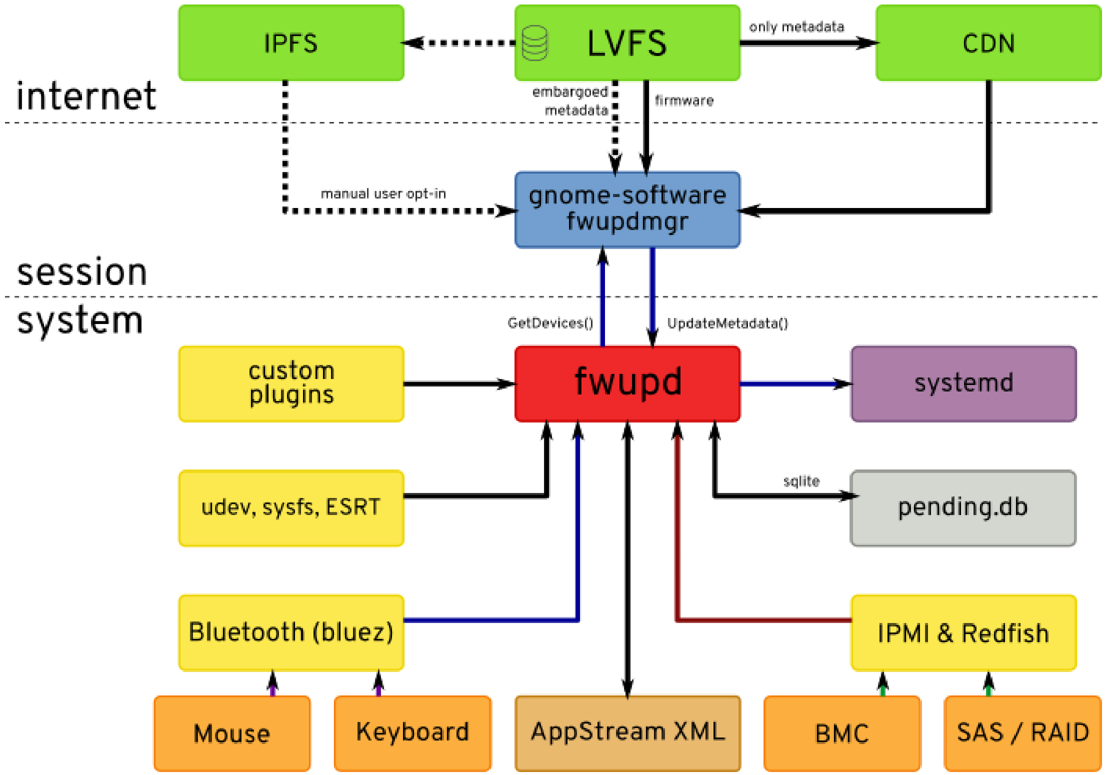
fwupd : Mechanism

The open source fwupd project deploys the update onto the Linux client machine. Over 32 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

Architecture



D-Bus is used to interact with fwupd

- Desktop neutral interface with binding for every language

Updates not applied without an agent

- Full integration with GNOME and KDE, with CLI interface
- Work on Cockpit and CoreOS integration for server

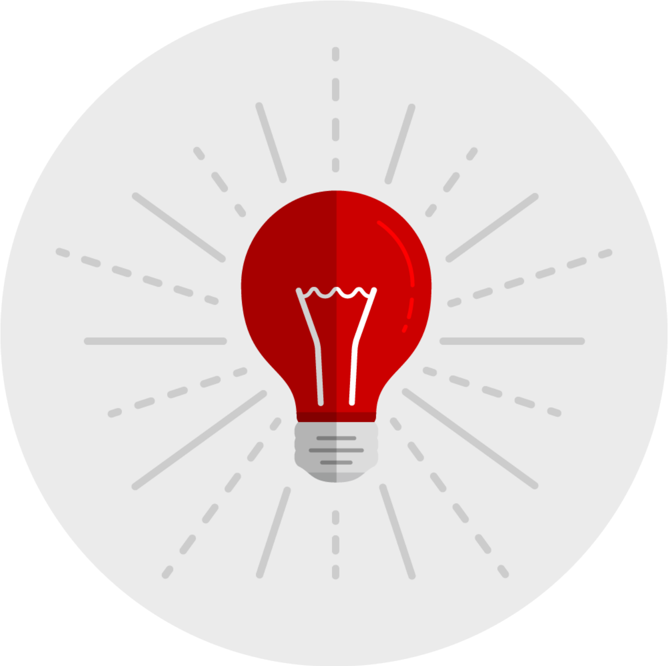
Scalable architecture designed to continue to grow

- LVFS hosted on AWS

Designed to the decentralised

- Can easily be mirrored on a private network and puts privacy first by matching hardware client side

The fwupd daemon will not run non-free code



Efficiency
Plugins enumerate and flash hardware, abstracting functionality as reusable modules. Typically ~1000 lines of code and easy to write and audit.

Maintenance
Hardware vendors do not need to build update binaries for many different Linux distributions.

Update protocol
Not be part of the device security protection. Use strong cryptography to prevent modification.

Compliance
Various customers are unable to run non-free static binaries from hardware vendors.

Every day over 15 million Linux users automatically download firmware update metadata from the LVFS.

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.

54.8M

Firmware files supplied to end users

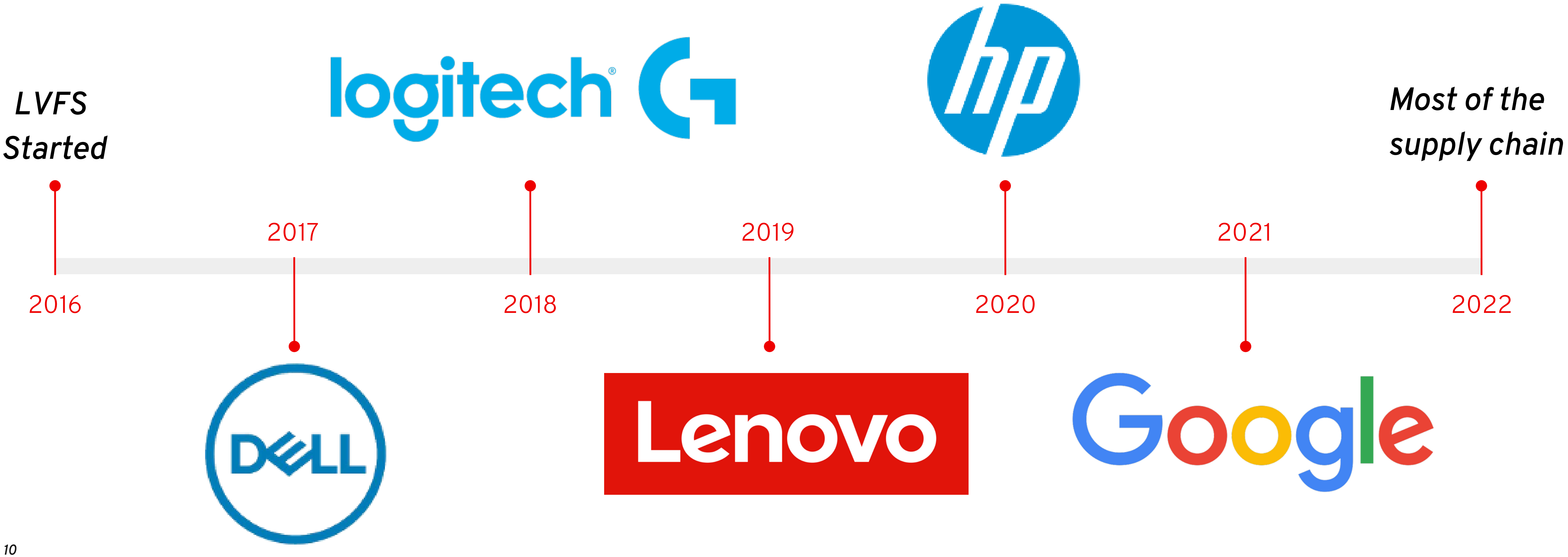
Since the LVFS started the official server has supplied millions of firmware updates for over 200 different devices.

176K

Success reports from end users

Over 99.97% of firmware was deployed correctly, with “known failures” identified using a built-in rule engine.

Over 150 OEMs, ODMs, IBVs and IHVs use the LVFS



LVFS Started

2016

2017

2018

2019

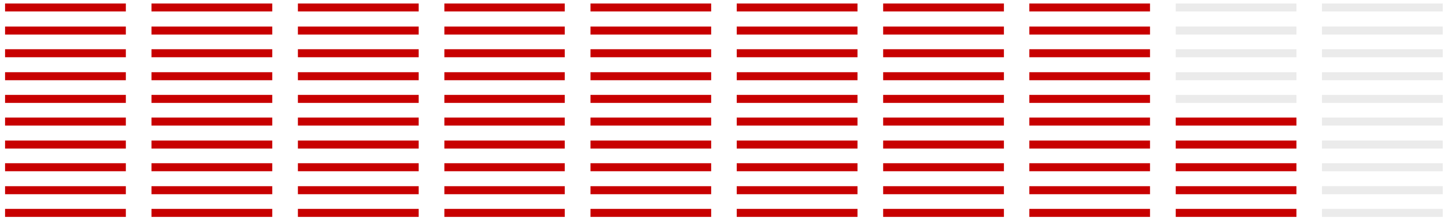
2020

2021

2022

Most of the supply chain

Server vendors are racing to get firmware on the LVFS



Lenovo ThinkSystem

The SR630v2 system has passed validation and the first firmware will be available on the LVFS 2022Q3 which puts Lenovo on several preferred supplier lists. More SKUs are expected by 2023.

Dell Server

One of the biggest customers has told Dell to **“Get on the LVFS”**. Dell is now certifying the Redfish plugin on 15th generation PowerEdge servers.

IBVs, ODMs and OEMs all work together

American Megatrends

Independent BIOS Vendor

The OBV typically uploads firmware to the LVFS to run tests and to verify that the image works with fwupd. IBVs and ISVs are normally not shown on the LVFS.

wistron

Original Device Manufacturer

The ODM can either just upload updates on behalf of the OEM, or the ODM can manage the entire QA process including pushing to testing and stable.

ThinkStation

Original Equipment Manufacturer

The OEM is the “user visible” brand the user is familiar with, and is typically the only vendor visible on the LVFS. OEMs can test firmware uploaded by their ODMs.

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...

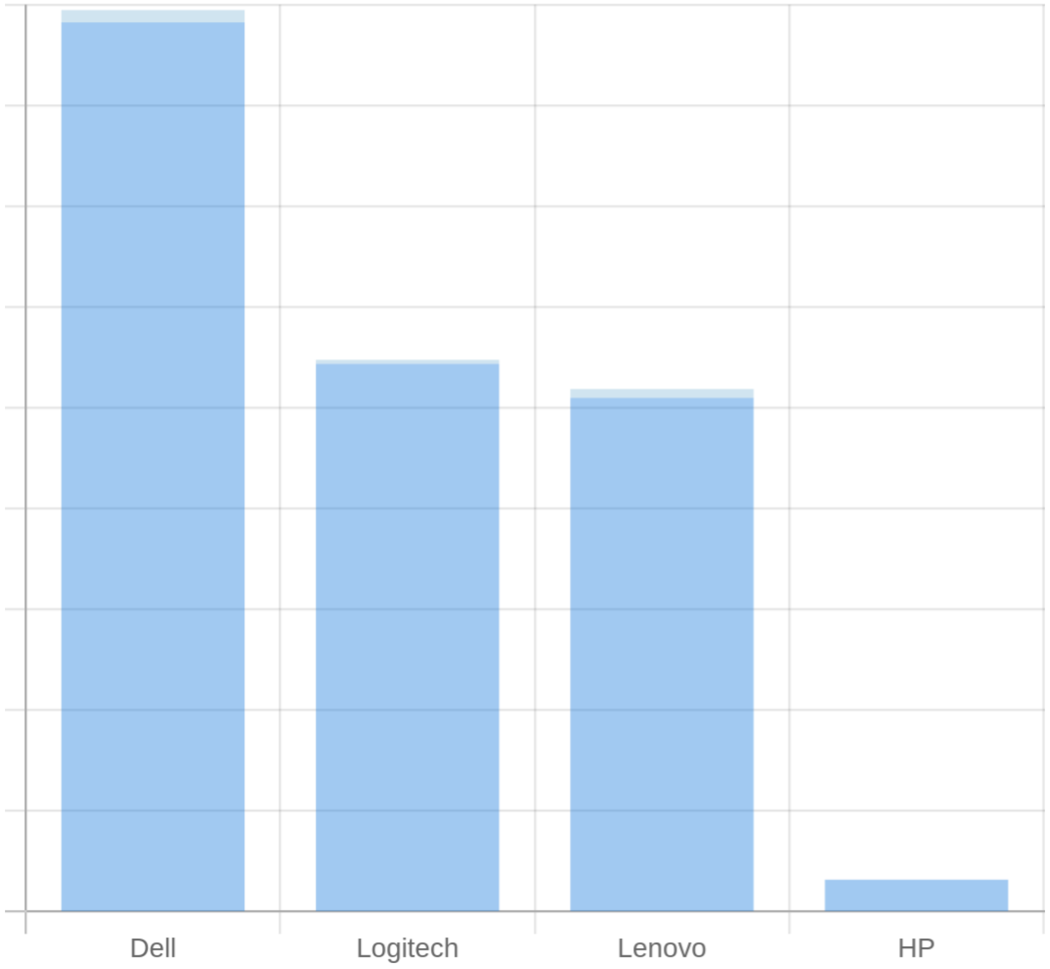
> “LVFS is strategically important for Dell to be able to provide secure firmware updates in a standards-compliant way.”

Mario Limonciello
Sr. Principal Software Engineer, Dell

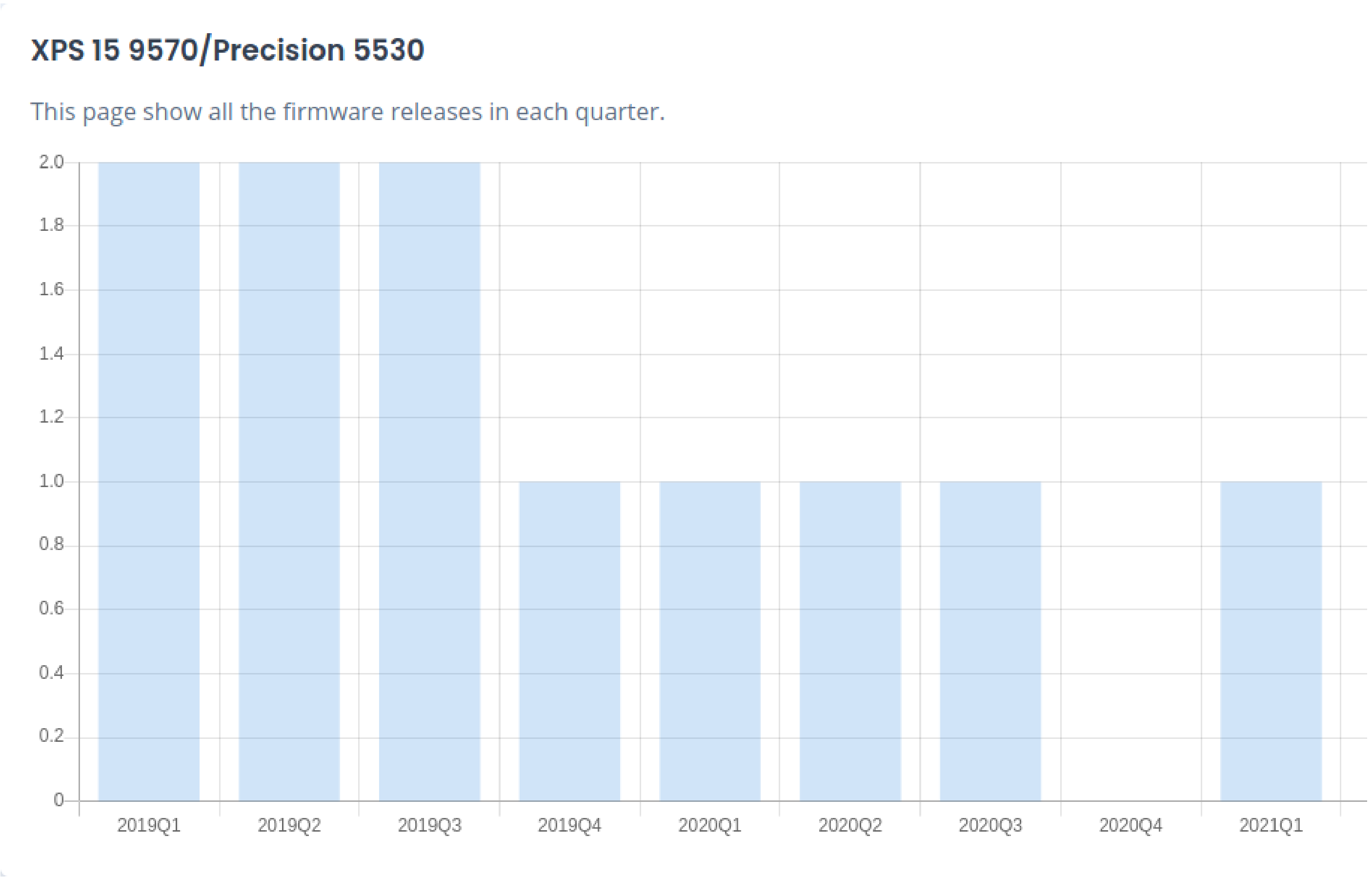
> “Standardizing on LVFS has helped Lenovo seamlessly distribute our firmware updates to our customers”

Rob Herman
Executive Director, Lenovo

Number of downloads, per vendor



Firmware update cadence used for purchasing



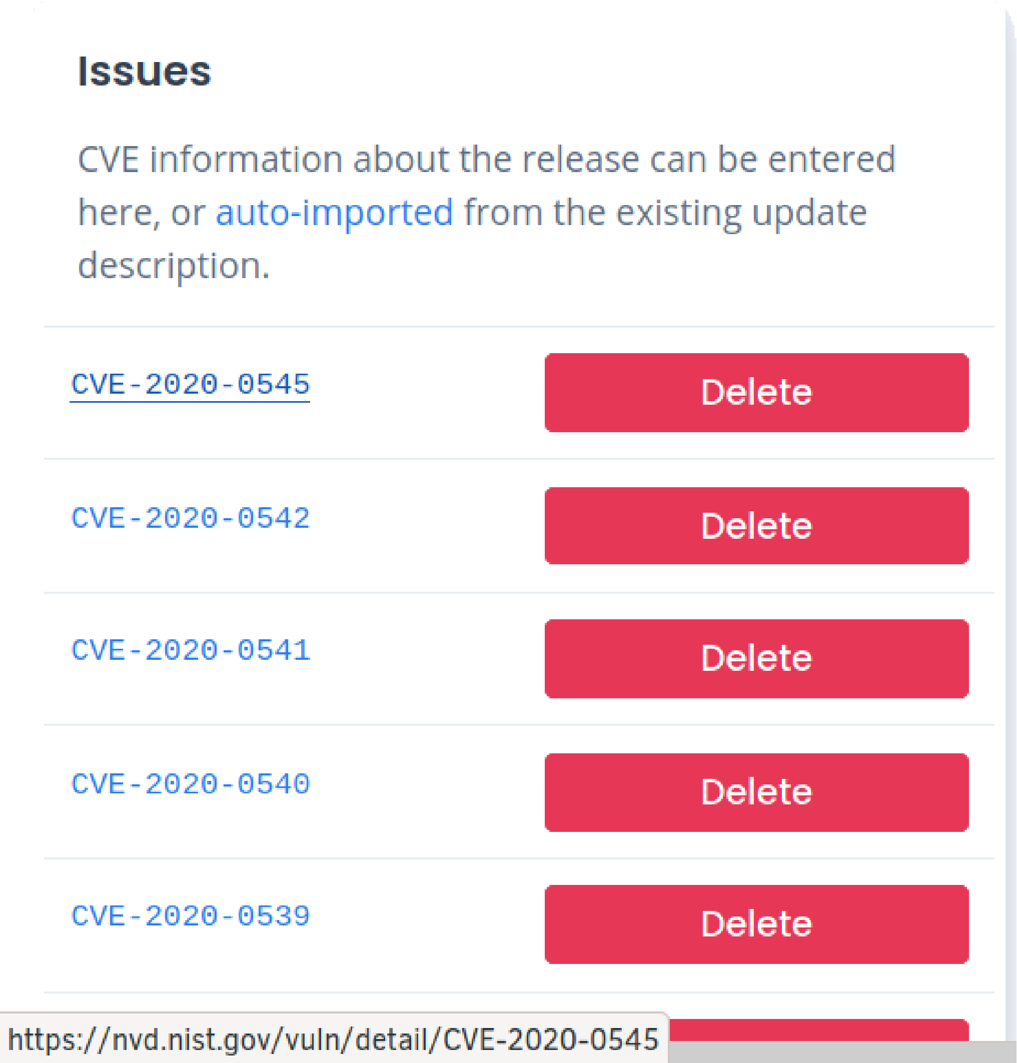
XPS 15 9570/Precision 5530

This page show all the firmware releases in each quarter.

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



Issues

CVE information about the release can be entered here, or auto-imported from the existing update description.

CVE-2020-0545	Delete
CVE-2020-0542	Delete
CVE-2020-0541	Delete
CVE-2020-0540	Delete
CVE-2020-0539	Delete

https://nvd.nist.gov/vuln/detail/CVE-2020-0545

2019

LVFS analyses uploaded firmware

Firmware is checked and scanned for known issues. Headers and footers are checked against the provided metadata values.

2020

LVFS helps secure the ecosystem

UEFI firmware is decompressed and analysed. Researchers can scan for vulnerabilities using Yara. Notification of microcode downgrade.

2021

LVFS launches HSI specification

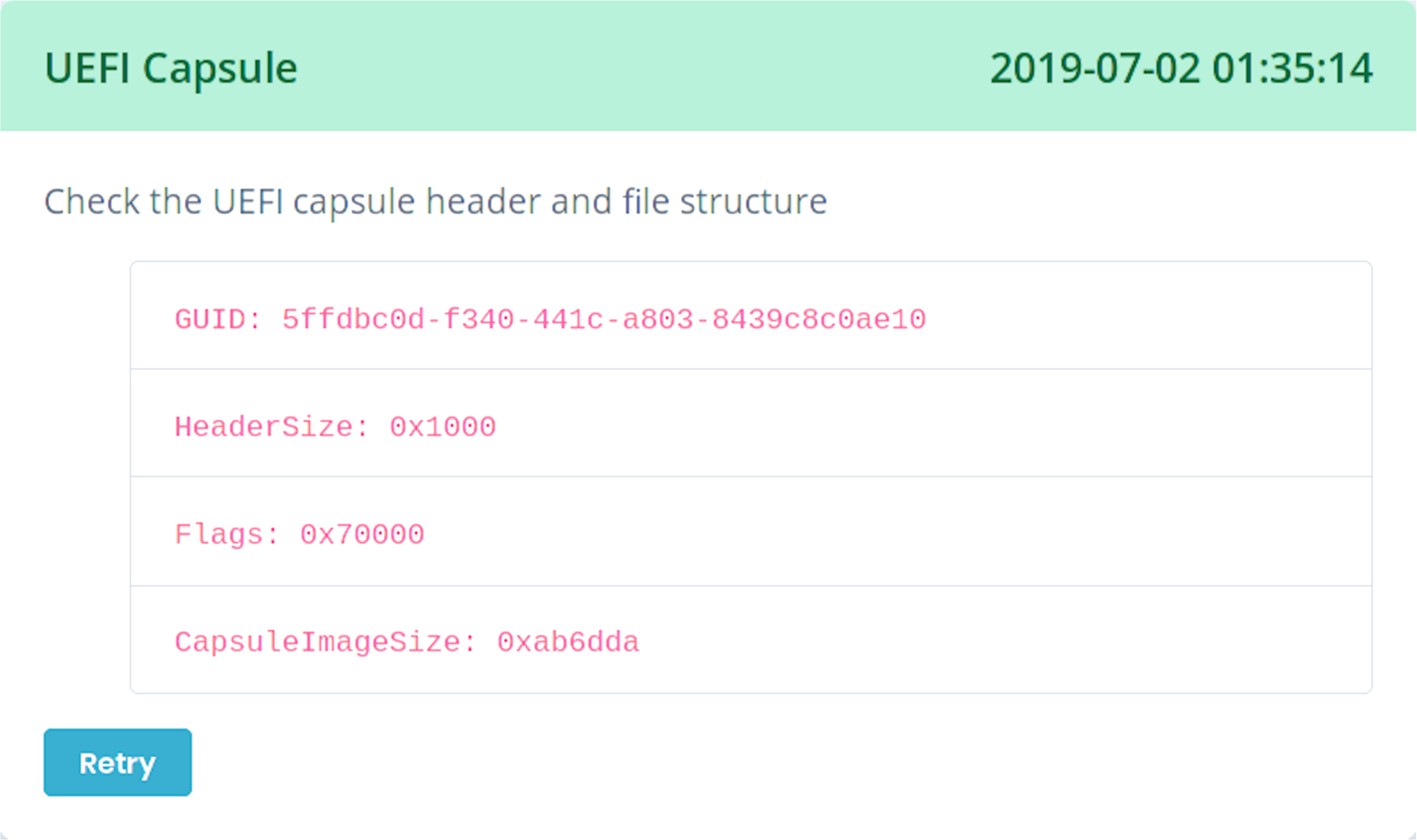
The Host Security ID indicates the level of platform security. Results are uploaded to LVFS for analysis. HSI will be used for purchasing decisions.

2022

LVFS launches fwupd friendly firmware specification

We want to make it easy for ODMs and OEMs to choose components that already have fwupd plugin support.

Firmware Analysis : UpdateCapsule

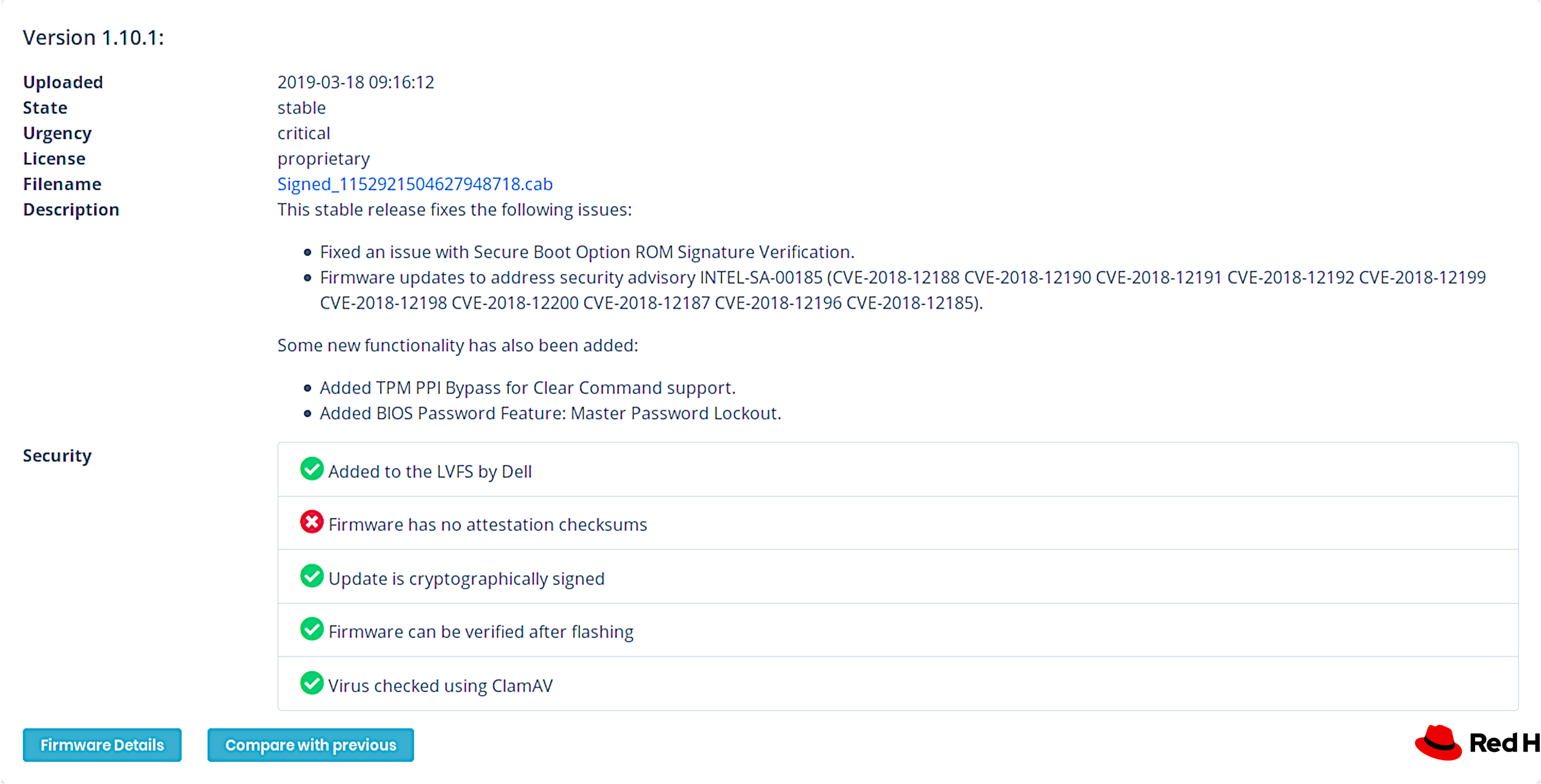


UEFI Capsule 2019-07-02 01:35:14

Check the UEFI capsule header and file structure

```
GUID: 5ffdbc0d-f340-441c-a803-8439c8c0ae10
HeaderSize: 0x1000
Flags: 0x70000
CapsuleImageSize: 0xab6dda
```

Firmware Analysis : Comparing Shards



Version 1.10.1:

Uploaded 2019-03-18 09:16:12

State stable

Urgency critical

License proprietary

Filename Signed_1152921504627948718.cab

Description This stable release fixes the following issues:

- Fixed an issue with Secure Boot Option ROM Signature Verification.
- Firmware updates to address security advisory INTEL-SA-00185 (CVE-2018-12188 CVE-2018-12190 CVE-2018-12191 CVE-2018-12192 CVE-2018-12199 CVE-2018-12198 CVE-2018-12200 CVE-2018-12187 CVE-2018-12196 CVE-2018-12185).

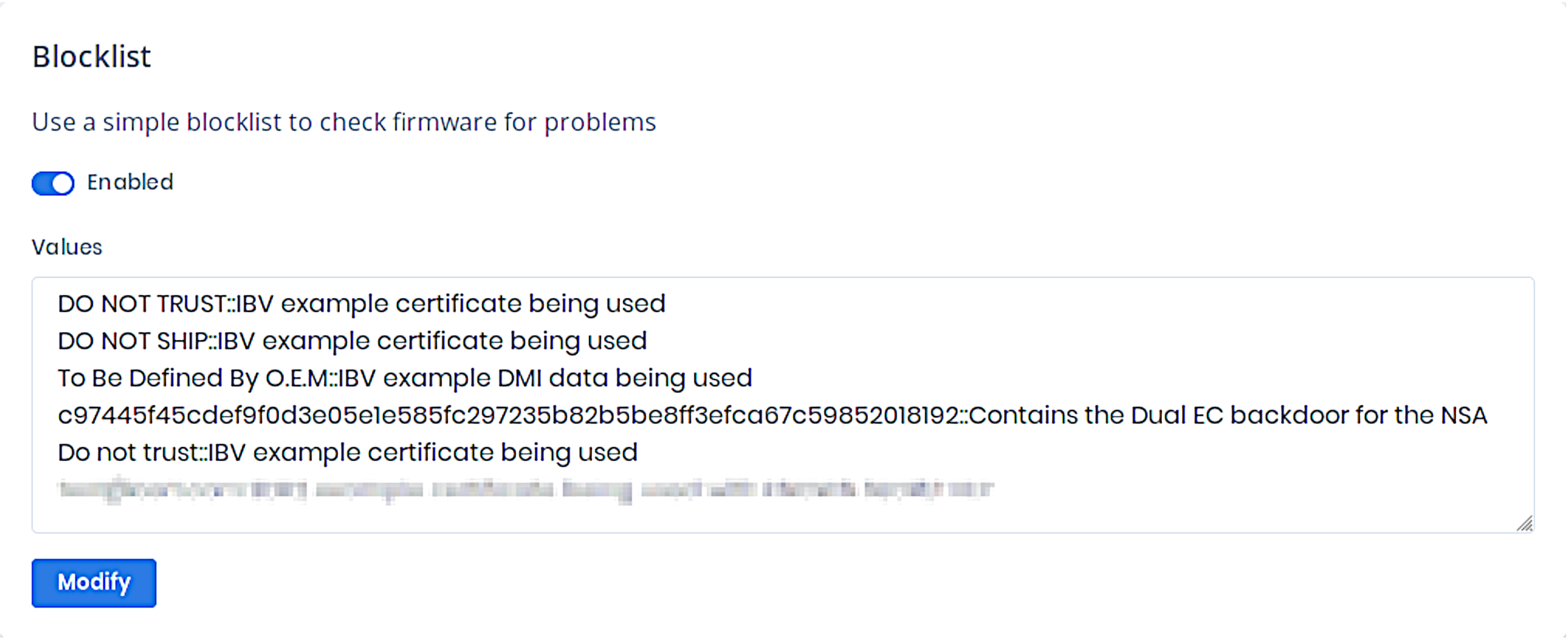
Some new functionality has also been added:

- Added TPM PPI Bypass for Clear Command support.
- Added BIOS Password Feature: Master Password Lockout.

Security

- ✓ Added to the LVFS by Dell
- ✗ Firmware has no attestation checksums
- ✓ Update is cryptographically signed
- ✓ Firmware can be verified after flashing
- ✓ Virus checked using ClamAV

Firmware Analysis : Raising the Bar



Blocklist

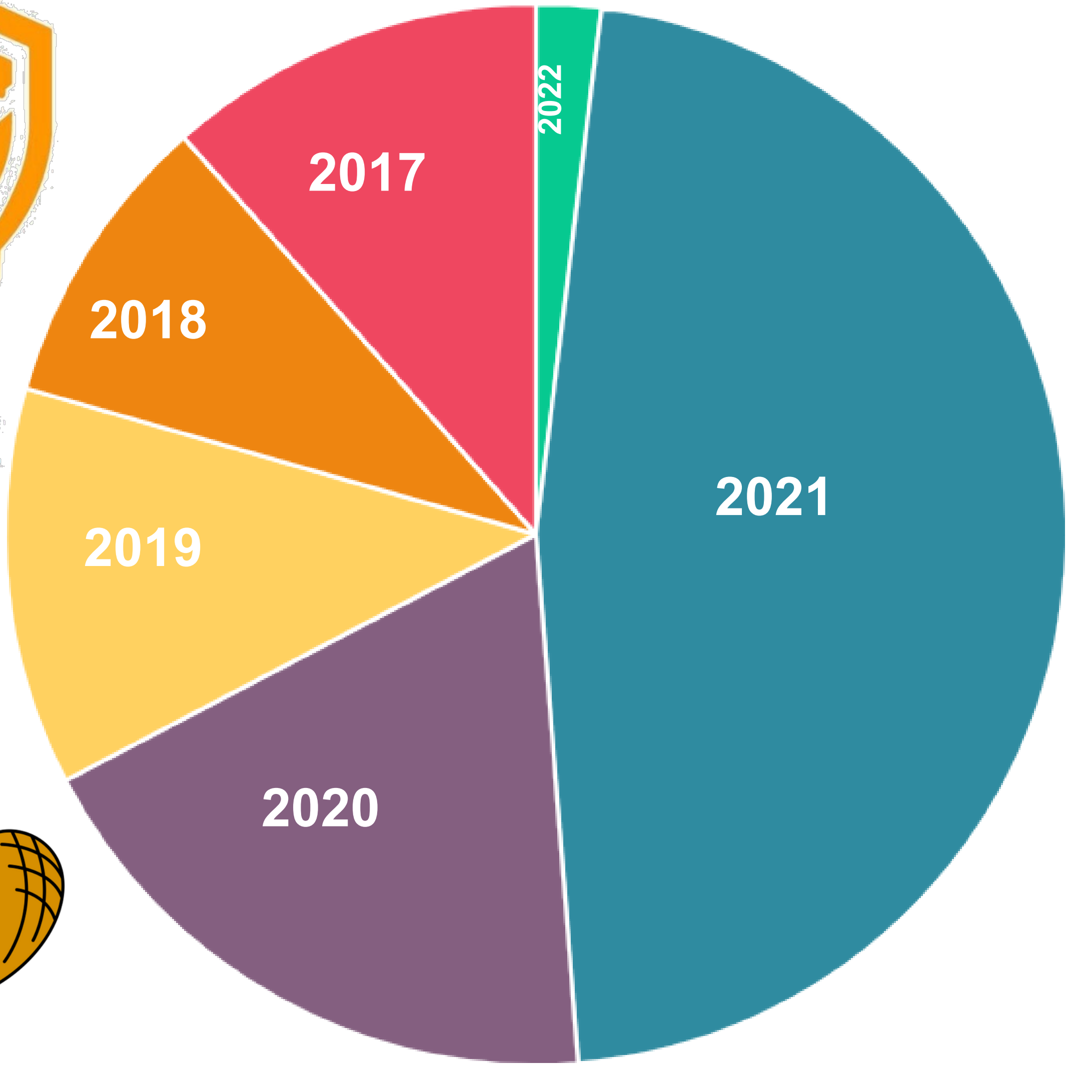
Use a simple blocklist to check firmware for problems

● Enabled

Values

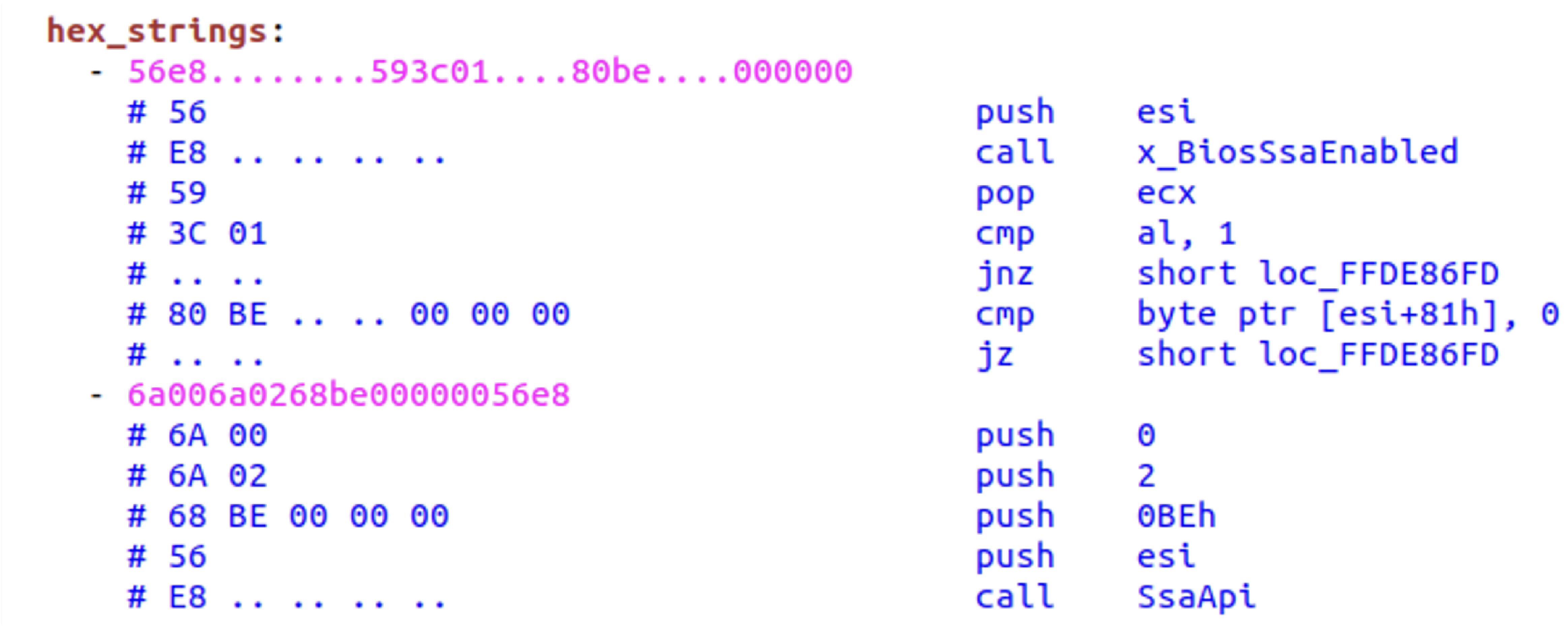
```
DO NOT TRUST::IBV example certificate being used
DO NOT SHIP::IBV example certificate being used
To Be Defined By O.E.M::IBV example DMI data being used
c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192::Contains the Dual EC backdoor for the NSA
Do not trust::IBV example certificate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

The newest versions of Intel Microcode



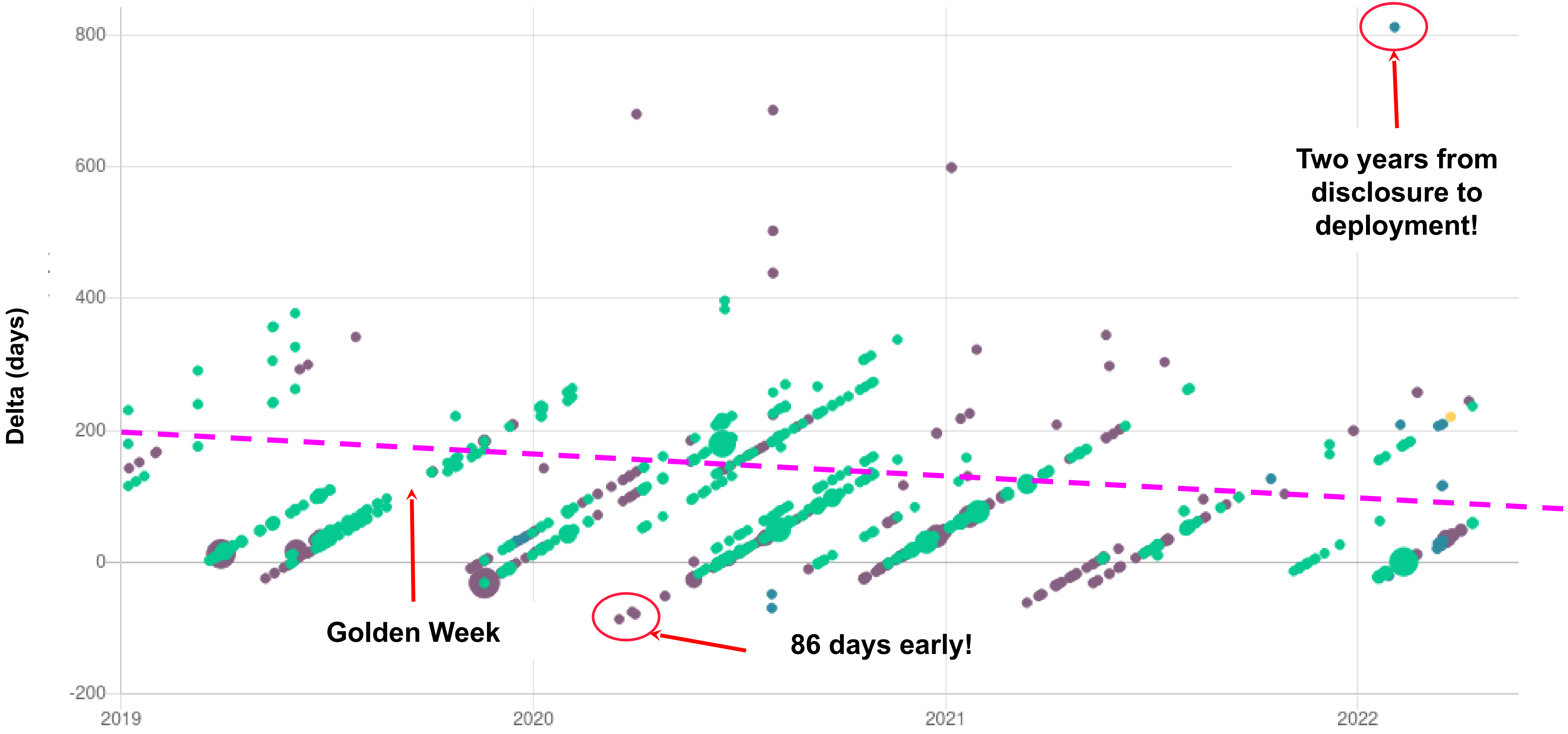
CVE-2022-21151 Processor Speculative Cross Store Bypass Advisory

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
```

Vendors take a long time to roll out fixes



Two years from disclosure to deployment!

Golden Week

86 days early!

Host Security ID provides clear and unambigious validation of firmware platform security

The HSI tests are performed at runtime during every system boot with no extra tools or configuration required.

By the OEM

The OEM can use the HSI tests to verify the claims of the hardware vendor or the independant silicon vendor.

By the corporate security team

The company or government security team can use the HSI specification to verify all hardware is running with the apropriate HSI value for the appropriate threat level.

By the user

The end customer can test the hardware in the field to test the OEM claims, and also check for firmware regressions after each upgrade.

Making firmware platform security simple

Assigning weights

We assign weights to various protections, e.g. `BIOSWE` (HSI:1) more important than TME (HSI:3)

Allow overrides

Security protections are allowed to obsolete other failures, for example BiosGuard obsoletes PRx register configuration

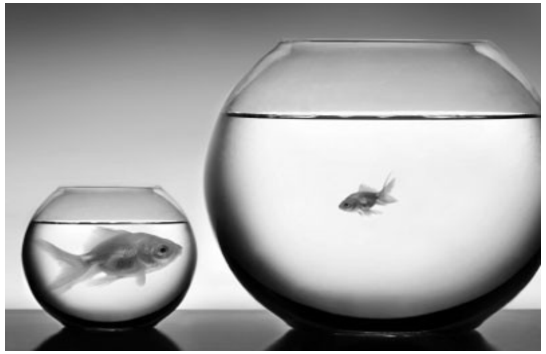
Secure by default

HSI forces vendors to turn on security by default out of the box as users do not manually run tests.

Test Specificacy

HSI tests can be silicon vendor or platform specific as requried. Higher HSI levels must pass **all** lower HSI tests.

Publishing the results make vendors aim higher

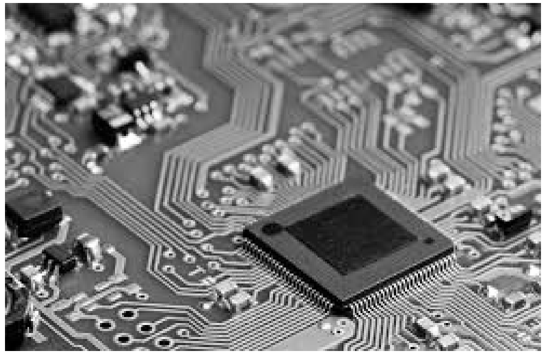


Public Scoreboard

A per-vendor and per-model public scoreboard allows consumers to check hardware before purchase and also compare OEMs and modes.

Purchase Requirements

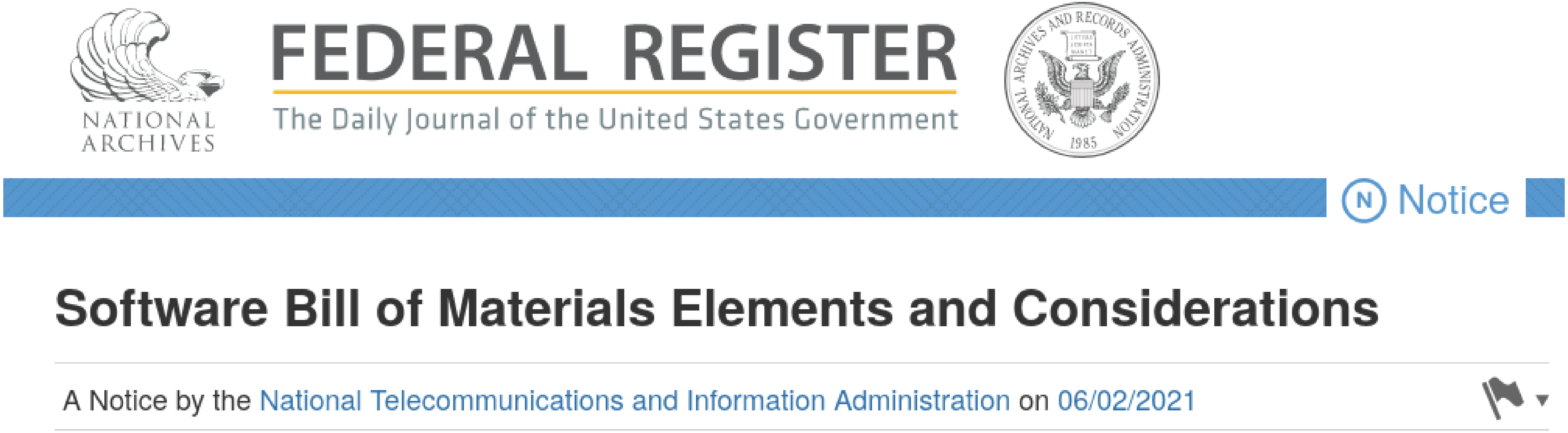
A minimum HSI level should be part of purchasing or bidding requirements for large contracts.



OEMs choosing secure hardware

Vendors should be chosing hardware based on price and how it affects the HSI value.

U.S. DoC says we have to care about SBoM



NATIONAL ARCHIVES

FEDERAL REGISTER

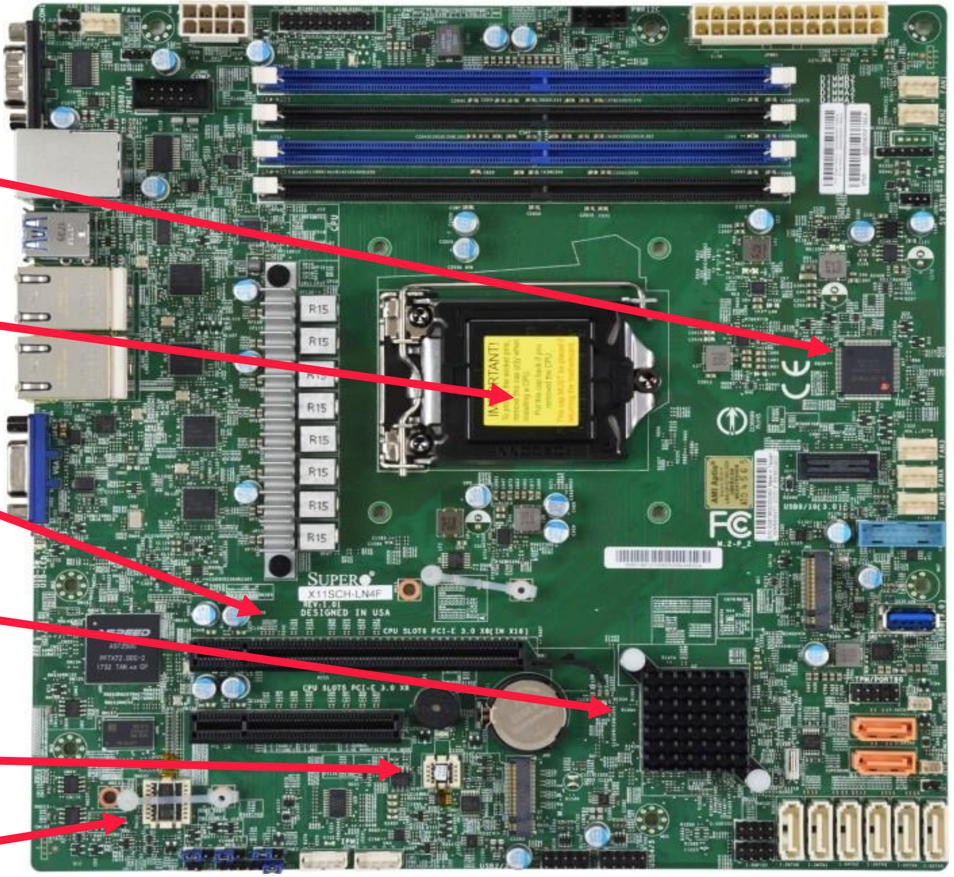
The Daily Journal of the United States Government

Notice

Software Bill of Materials Elements and Considerations

A Notice by the National Telecommunications and Information Administration on 06/02/2021

We have more than one blob?



FPGA firmware

Intel microcode & FSP

PCI option ROMs

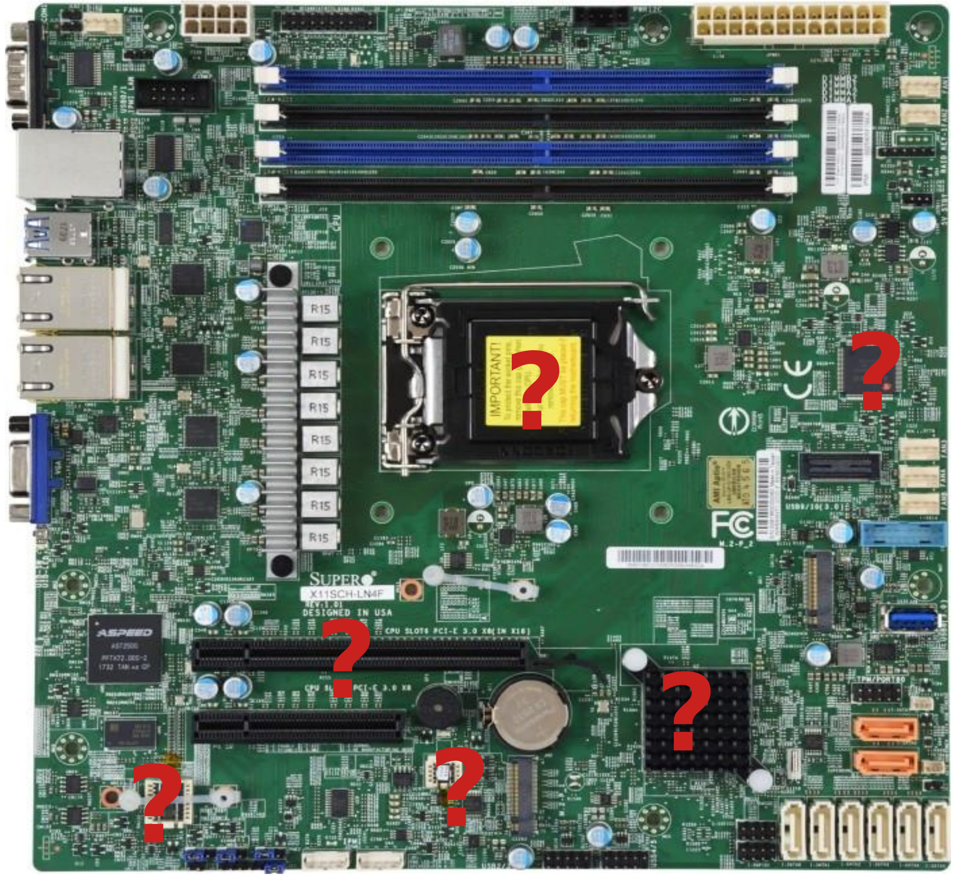
Southbridge firmware

LinuxBIOS

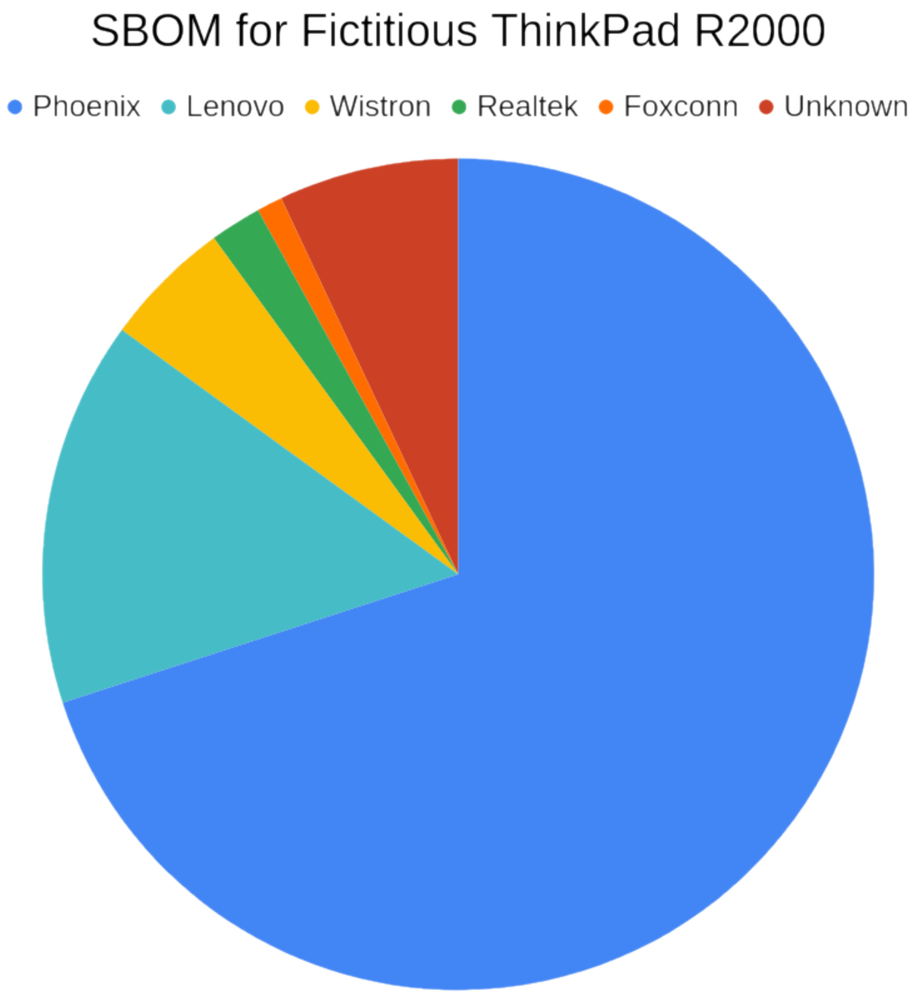
BMC firmware

Who supplied each firmware?

- Who built them?
- When did they build it?
- What OpenSSL did they use?
- What is the licence?
- What is the version?
- What were the file hashes?



SBOM via uSWID



Embed the SBOM data into a SBOM COFF section

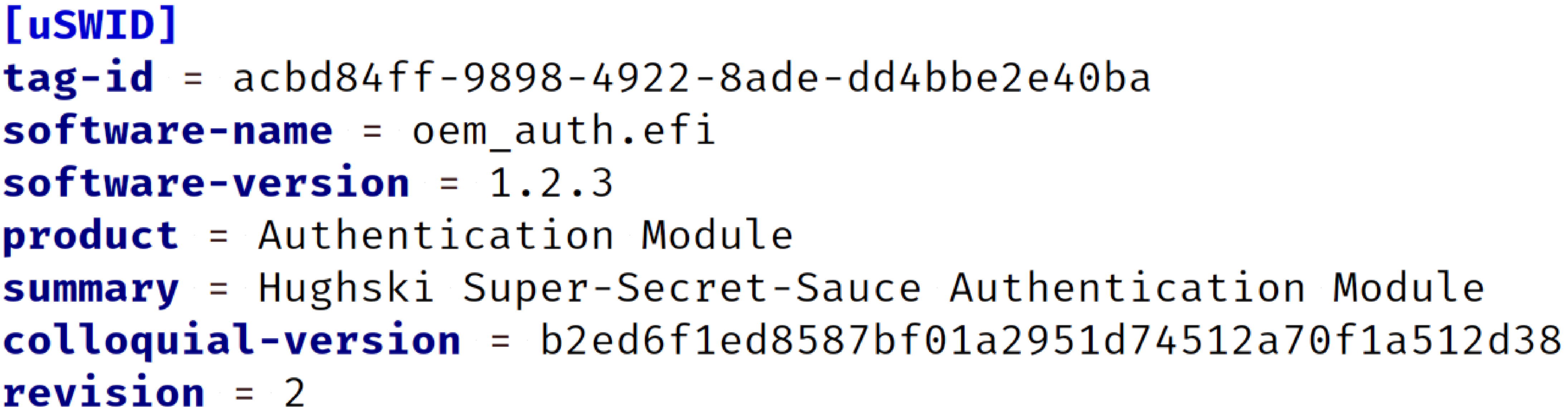
- Means it doesn't get stripped
- Means we need to teach AV scanners
- Which allows the LVFS to extract from FVs

Allow entity "patching" using a simple .ini format

```
[uSWID-Entity:Distributor]
name = OEM Vendor
```

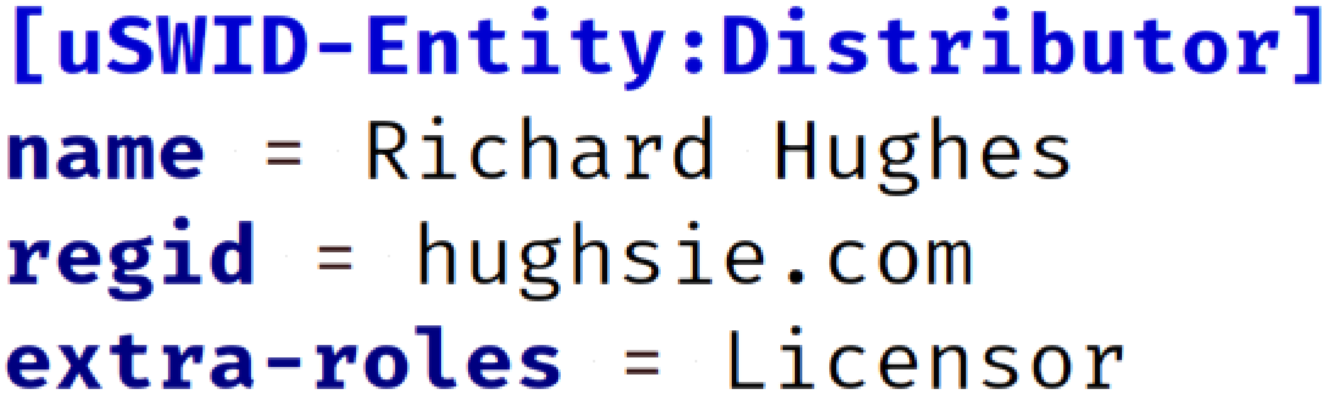
https://github.com/hughsie/python-uswid

IBV Metadata



```
[uSWID]
tag-id = acbd84ff-9898-4922-8ade-dd4bbe2e40ba
software-name = oem_auth.efi
software-version = 1.2.3
product = Authentication Module
summary = Hughski Super-Secret-Sauce Authentication Module
colloquial-version = b2ed6f1ed8587bf01a2951d74512a70f1a512d38
revision = 2
```

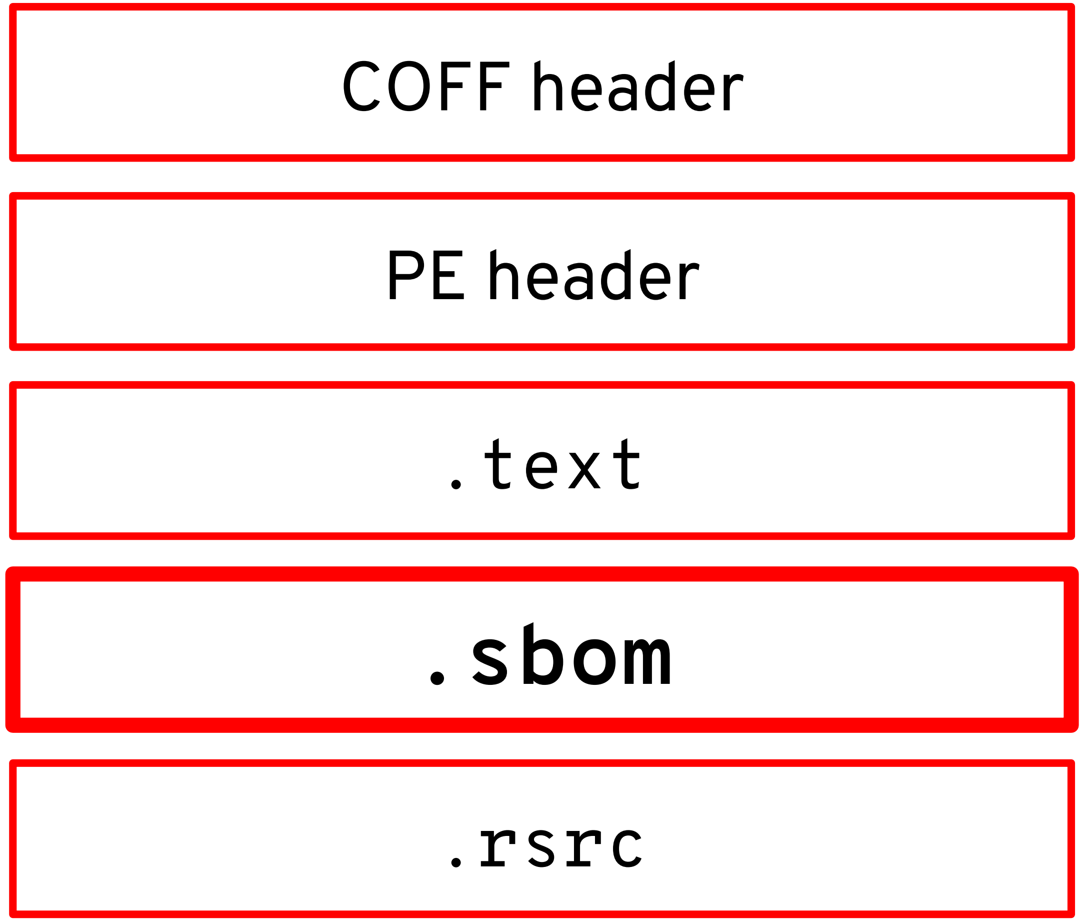
ODM & OEM Metadata



```
[uSWID-Entity:Distributor]
name = Richard Hughes
regid = hughsie.com
extra-roles = Licensor
```

```
$ pip install uswid
$ uswid --inifile oem.ini --binfile ./odm_auth_NEW.efi
```

A New COFF Section for EDK2



COFF header

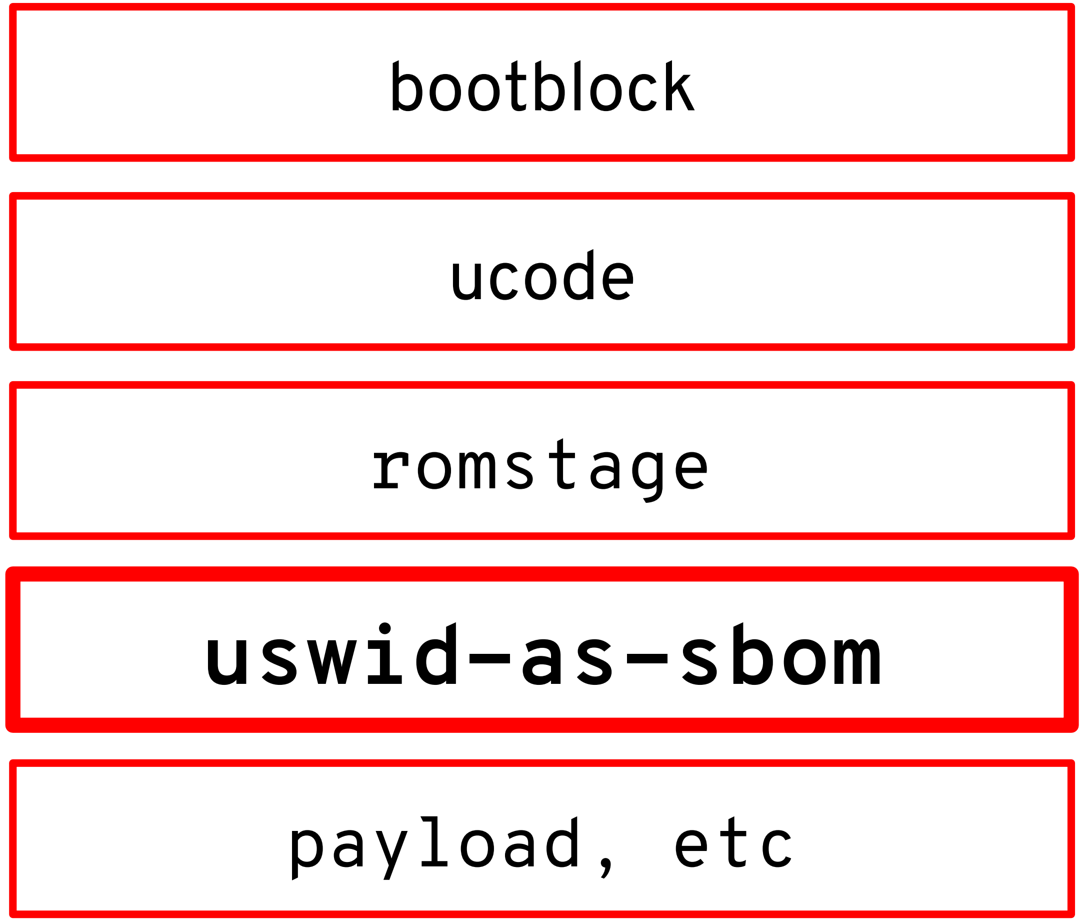
PE header

.text

.sbom

.rsrc

A New CBFS section for coreboot



bootblock

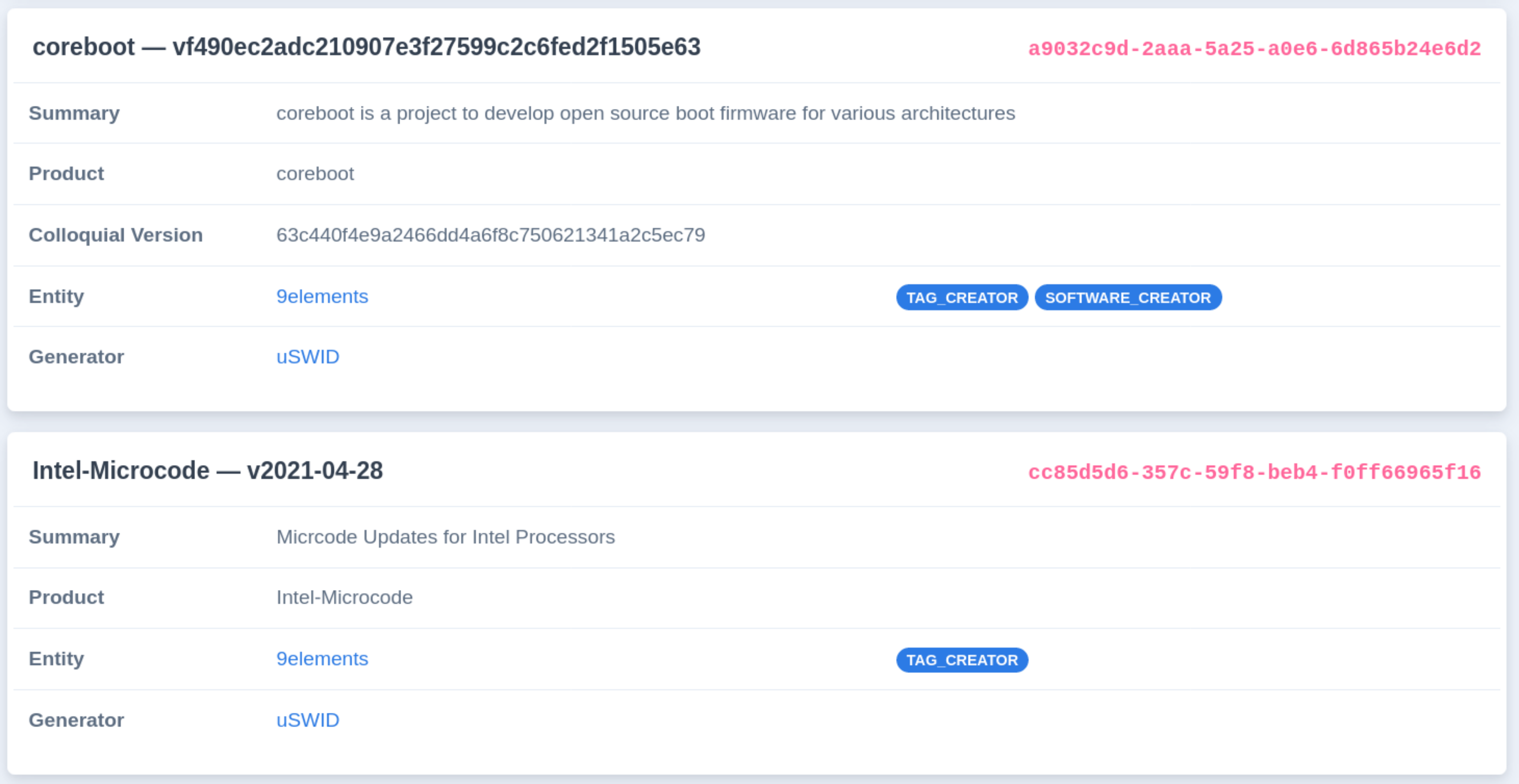
ucode

romstage

uswid-as-sbom

payload, etc

LVFS end-to-end with SWID 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	

Call to action

What we should do:

- Talk to people about what LVFS is trying to do.

- Work with OEMs like Lenovo, Dell, Intel and AMD on HSI checks.

- Make LVFS part of government and commercial purchasing requirements.