github.com /rhboot/shim/issues/685

SBAT: Shim repository should provide a parsable SbatLevel.txt for external automated tools and workflows · Issue #685 · rhboot/shim

rhboot ⋮ 5-6 minutes

Summary:

Just like there is a public central authority publicly providing the latest global DBX(s) (https://uefi.org/revocationlistfile), Shim should provide a **single** up-to-date global SBAT, containing the very latest SBAT versions for each vulnerable product, that could then be referenced by system maintainers as well as automated external tools and workflows.

We believe that the current `SbatLevel_Variable.txt` does not fit that purpose as it is:

- not processable by automated tools
- not authoritative, in that it provides different versions for the same product, and asks the SBAT "reader" to choose which one it wants to use.
- potentially subject to deletion or renaming, on account of being documentation corollary, rather than a crucial, immutable, resource.

We therefore propose that Shim should have an authoritative, machine processable, `SbatLevel.txt`, at the root level of this project, containing the most up to date versions, so that workflows that want to use SBAT to filter out currently known vulnerability, can use that authoritative reference.

Context

In their latest Windows update (KB5041585 for Windows 11, but more specifically mentioned in KB5041160) Microsoft took it upon themselves to update the SBAT on all updatable systems that are under their control.

They did so using this exact data (retrieved from a Windows 11 system where the update had been applied, from `C:\Windows\System32\SecureBootUpdates\SbatLevel.txt`, which is the source used by Windows for SBAT UEFI variable update):

```
sbat,1,2024010900
shim,4
grub,3
grub.debian,4
```

As has been reported here, this leads to issues such as #682 as well as related issues, such as the inability to boot the latest Ubuntu installer.

Obviously, and this is not our issue, we believe it is an OS manufacturers' call to update Secure Boot related variables as they see fit, to mitigate or prevent reported vulnerabilities.

However, as the developers of a popular Windows application (Rufus), that can be used to create GNU/Linux installation media, and in light of the woes experienced by Linux users after this Microsoft update, we would very much like to parse the SBAT of UEFI bootloaders from media we create, so that we can pre-emptively alert the user in case they use one that will be deemed vulnerable, in a manner similar to how we already check UEFI bootloaders hashes against the latest DBX, and will warn the user if we find a revoked bootloader.

To be able to do that for hash revocation, we can simply automate the download and parsing of the latest DBX from https://uefi.org/revocationlistfile.

However, in its present form, we can not really (easily) do the same for https://github.com/rhboot/shim/blob/main/SbatLevel_Variable.txt as this data is more of a documentation entry aimed at being read by humans than an authoritative, machine processable, data source. It is also very unclear/uncertain whether that `SbatLevel_Variable.txt` may not disappear from one day to the next, if it is renamed or moved around in the repo, as documentation is wont to do, thus breaking any automated tool and process that may depend on it, such as system maintainers who are likely to want to use it to automate the update of their SBAT variables.

We therefore urge RH Shim to introduce a single `SbatLevel.txt`, at the root of this repository, that would include only the latest SBAT versions (possibly with some comments, as long as they are prefixed with something that automated tools can filter out like #), and declare it authoritative and up-to-date, so that people can both reference it as the official current SBAT version, and so that automated processes and workflow can start to make use of it.

Or, if we believe that there might be a need for different "Reported" and "Fixed" SBAT version lists, in case system maintainers want to have the choice of blocking vulnerabilities as soon as they are reported vs. only when there does exist a replacement non-vulnerable bootloader, RH Shim may also introduce a dual set of `SbatLevel_Reported.txt` as well as an `SbatLevel_Fixed.txt` authoritative files...

At any rate, just like there exists a central, immutable, https://uefi.org/revocationlistfile, that people and workflows can reference to as **the** central authority to obtain the latest DBX updates, we believe there needs to be a better location than `SbatLevel_Variable.txt`, that people and workflows can reference to as **the** central authority to fetch the most up to date SBAT UEFI variables.