VERITAS
The truth in information.

2625 Augustine Drive,
Santa Clara CA 95054

Response of Veritas Technologies LLC (“Veritas”) to Draft NIST White Paper Baseline Criteria for Consumer Software Cybersecurity Labeling December 16, 2021

Section 2.3.1.2 Label Scope

It should be made clear that the label scope needs to be for an entire product, not for a portion of a product. For example, a vendor should not be able to limit the scope to an application that they put on top of a version of Linux that they distribute and then say that their application has no known vulnerabilities, while ignoring the underlying Linux distro. That could give consumers a very misleading idea of the security of the product.

Section 2.3.1.5 Software End of Support Date

It seems like this section needs to be more constrained. If a consumer is told that software is supported through some date then it seems that there should be some sort of obligation that the vendor has to actually provide software updates to address vulnerabilities. A consumer might reasonably assume that if no updates are available that there are no known security issues with the software, when in fact the vendor knows of dozens of issues but has chosen to not release an update.

Section 2.3.3.1 Free from Known Vulnerabilities

We suggest two additional points be made in this section:

- There should be some sort of statement that the vendor has made reasonable efforts to find vulnerabilities in the product. It’s much easier to not know of vulnerabilities if you never look for them.
- It should be clarified that this means that the product was free of known, ***exploitable*** vulnerabilities as of the attestation date. If a vulnerability in a third-party component cannot be exploited from the product then it should not be considered a “known vulnerability” for this field.

Section 2.3.3.2 Software Integrity and Provenance

The description states “The software and all provided updates are cryptographically signed by ***the software provider***.” There could be issues doing this with proprietary third-party software that is included by the software provider that was signed by the third party. We suggest considering that all software and updates be cryptographically signed without limiting the signing exclusively to the software provider. While this isn’t ideal, we think it’s better than not making any claim at all.

Section 2.3.3.5 Strong Cryptography

- Limiting the label to only NIST approved cryptography seems overly restrictive. For example, software may include support for TLS 1.3, which can include ChaCha20/Poly1305 and neither of those are NIST approved as of today. It would be unfortunate to exclude such implementations, so we propose providing a second label such as IETF. This would mean that as of the attestation date that all cryptography was compliant with the most recent IETF RFCs related to the cryptography included in the product. While adding a second possible value is somewhat undesirable, giving consumers the impression that a product uses insecure cryptography when in fact it does not is more undesirable.

- We suggest there should be a text that this statement only applies to crypto used for a security purpose. It should not apply to crypto used for non-security purposes, e.g. a random number generator used to generate data for a game.

Submitted By

David Dillard
Technical Director, Product Security Group
Veritas Technologies LLC