

Freigabe einer Fremdbibliothek

Die Freigabe einer neuen Fremdbibliothek von oben nach unten. Die ersten fünf Punkte beenden die Prüfung sofort, die weichen Kriterien darunter tragen nur zum Urteil bei.

Hart, jeder Punkt beendet die Prüfung

☐

Lizenz

Verboten oder unbekannt heißt Befund. Eine nicht nachweisbare Lizenz ist keine Freigabe.

☐

Name

Steht er auf der Sperrliste oder liegt er verdächtig nah an einem bekannten Paketnamen, ist Schluss.

☐

Bekannte Schwachstelle

Für die geprüfte Fassung liegt eine ungepatchte Lücke hoher Schwere vor.

☐

Quellcode

Es gibt kein öffentliches Quell-Repository. Was niemand lesen kann, prüft auch niemand.

☐

Alter

Das Paket ist jünger als 90 Tage.

Weich, jeder Punkt geht ins Urteil ein

☐

Wer schreibt daran

Kommen neun von zehn Commits von einer Person, ist das Projekt verwaist, sobald diese Person geht.

☐

Letzter Commit

Bei einem lebenden Projekt erwarten wir Aktivität in der letzten Woche. Bei einer ausentwickelten Bibliothek sind drei bis vier Monate in Ordnung. Jahre nie.

☐

Offene Meldungen

Alte Funktionswünsche dürfen liegen. Echte Fehler, älter als ein Jahr, sind ein Warnzeichen.

☐

Wer trägt es

Eine Stiftung im Rücken zählt. Mitarbeit unter Firmenkonten zählt. Aufnahme in den geprüften Teil einer großen Distribution zählt.

Vor dem Einbau

☐

Wartefrist

Neue Fassungen kommen 14 Tage zu spät ins Projekt, mit Absicht. Bei zwei untersuchten Angriffen auf Paketverzeichnisse waren die verseuchten Fassungen nur Stunden verfügbar.

☐

Protokoll

Jeder abgefragte Wert steht mit dem Zeitpunkt seines Abrufs in einer Datei im Repository. Danach fragt die Baustrecke nichts mehr ab, sie vergleicht nur noch.

☐

Ausgang

Aufnehmen, ablehnen, Ausnahme mit Unterschrift, oder forken und selbst pflegen. Eine Ablehnung, die man vergisst, wird beim nächsten Mal zur Aufnahme.



Eine unterschriebene Ausnahme mit Begründung und Namen hebt jeden dieser Befunde auf. Einen nicht: die Sperrliste.