SAFEGUARD GOLD · DATASHEET

Safeguard

Start from builds you can verify, and fix without waiting for upstream.

Gold has two parts: a free public directory of what is known about open-source software, and a registry of rebuilt, signed packages.

THE PROBLEM

Upstream maintainers do not always ship a fix quickly, or at all. Until they do, teams carry a vulnerable package or maintain a private patch. Public package indexes also say little about how an artifact was built, so you cannot check what you are installing.

WHAT IT DOES

Gold Open Source, free

gold.safeguard.sh needs no login. Look up a package or CVE, run the "Am I affected?" checker, or use the free read API.

Fix PR when a fix exists

When a fixed version exists, Safeguard opens a fix pull request that moves you to it.

Fix without waiting for upstream

When upstream has no fix yet or will not ship one, Safeguard works to get the fix accepted upstream.

Hardened build when needed

If the issue is severe or upstream will not move, Safeguard builds a fork, fixes it and publishes a hardened Gold build.

HOW IT WORKS

1. **Flag** — A vulnerable dependency appears in your inventory
2. **Fixed version?** — If one exists, a fix PR moves you to it
3. **Upstream** — If not, Safeguard works to get the fix accepted
4. **Fork and fix** — If severe or stalled, build a fork from source
5. **Sign and serve** — Signed Gold build with SBOM, provenance and VEX

GOLD REGISTRY

Safeguard Gold rebuilds patched versions of open-source packages and images from source, signs each build, attaches an SBOM, SLSA provenance and VEX, and serves them from registry.safeguard.sh to your organization.

CAPABILITIES IN DETAIL

Directory contents	Packages, container images, CVEs, CWEs, MITRE ATT&CK, AI models, MCP servers and agent skills, searchable without an account.
Am I affected?	Check a package and version against known vulnerabilities and get a recommended safe version.
Gold Certified label	In the free directory, a component is Gold Certified when no vulnerabilities are known in the indexed version and it is not deprecated.
Free access	Read API, Chrome extension for lookups from the browser, and a CI gate action that can fail a build on KEV or known vulnerabilities.
Registry builds	Patched versions rebuilt from source and served to your organization. Each build is signed.
Build evidence	SBOM, SLSA provenance and VEX attached to each Gold build.
Fix route	Fix PR if a fixed version exists, upstream contribution if not, fork and hardened build if severe or stalled.

INPUTS

- A package name and version, or a CVE ID
- A container image
- Your dependency inventory (for registry builds)
- A request for a patched package

OUTPUTS

- Known vulnerabilities, fixed versions, safe version
- Fix pull request
- Signed patched build
- SBOM, SLSA provenance and VEX

INTEGRATIONS AND SURFACES

npm · PyPI · Maven · Go · Cargo · RubyGems · Composer · NuGet · Chrome extension · Free read API · CI gate action · Safeguard CLI

DEPLOYMENT AND DATA HANDLING

Open Source directory
Free, no login. Look up a package or CVE without an account.

Registry delivery
Gold builds are served to your organization. Contact us about private VPC, on-prem and air-gapped delivery.

Regions and hosting
SaaS in US, EU (Frankfurt) and Gov regions. Private VPC, on-prem and fully air-gapped deployments are available.

Access control
SSO (SAML 2.0, OpenID, Google, Microsoft, GitHub), roles and 2FA.

Look up a package on Gold

`gold.safeguard.sh`

Scan the code or type the address. Questions: hi@safeguard.sh

Safeguard

SOC 2 Type I and Type II audited; reports available on request (safeguard.sh/trust). Designed for FedRAMP High.