Cribl

>WHITE PAPER_

Cribl’s blueprint for secure software development:

Integrating security at every step.

>WHITE PAPER_

Cribl's blueprint for secure software development:

Integrating security at every step.

Cribl has the most security-conscious customers in the world, and building secure products is part of Cribl's engineering identity. We have built a secure software development lifecycle that is both culturally and policy driven, where product security tooling and processes are integrated into every architecture review, every pull request, and every major and minor release.

Cribl's software development lifecycle security program includes:

- Cribl's product security team.
- Compliance with the NIST Secure Software Development Framework (SSDF).
- Secure software development training.
- Security Champion program.
- Product security reviews.
- Securing the supply chain.
- Open Source Software (OSS) governance.
- Static Application Security Testing (SAST).
- Dynamic Application Security Testing (DAST).
- Vulnerability management.
- 3rd party penetration testing.
- Responsible disclosure.

Cribl's product security team.

Cribl has invested in a world class Product Security Team with over 80 years of combined software security development experience to ensure the programs detailed in this whitepaper are robustly maintained, effective, and highly auditable.

Compliance with the NIST Secure Software Development Framework (SSDF).

The NIST (National Institute of Standards and Technology) Secure Software Development Framework (SSDF) is a set of guidelines aimed at helping organizations establish a secure software development lifecycle (SDLC). The SSDF provides a comprehensive approach to ensuring security of software throughout its development process, from initial planning to deployment and maintenance. Cribl has implemented the full suite of practices and tasks as defined in the NIST SSDF 1.1 and can share a letter of third party attestation with customers at any time.

Secure software development training.

To ensure that Cribl's engineering teams are equipped with the knowledge and skills to build secure software and cloud architecture, role-based training in secure development practices is required at least annually.

Security Champion program.

Cribl Security Champions act as liaisons between the Product Security Team and the Engineering Teams. Cribl's Security Champions receive specialized security training to share with their respective teams. This helps in raising the overall security knowledge and awareness across Cribl. Security Champions also provide valuable feedback to the Product Security Team from a developer's perspective so that the programs detailed in this document are continuously improved.

Product security reviews.

Every engineering epic at Cribl includes tasks for rapid risk assessment and threat modeling. Threat modeling allows teams to identify potential security threats and their mitigations early in the development process. The threat mitigation output of every threat model is distilled into actionable engineering tasks which are completed to Cribl's definition of done.

Cribl Security Champions act as liaisons between the Product Security Team and the Engineering Teams raising the overall security knowledge and awareness across Cribl.

Securing the supply chain.

All Cribl products are built using a dedicated, hardened, and monitored continuous integration system. Cribl's source code is tracked in a centralized version control platform. Single sign on (SSO) with multi-factor authentication and least access privilege is enforced for all access to Cribl's continuous integration systems. All pull requests require peer review and approval before being merged into the production branch. All Cribl software build artifacts are signed. A strict separation of duties is enforced between the engineers that create code, maintain the build system, and promote the artifacts to production.

Open Source Software (OSS) governance.

Cribl's Product Security Team reviews all open source components and their transitive dependencies for vulnerabilities and operational and licensing risk. Leveraging Software Composition Analysis (SCA) software integrated with Cribl's code repository, an automated Software Bill of Materials (SBOM) is generated with each build of Cribl's software. An SBOM offers visibility into the software supply chain, enabling organizations to assess the trustworthiness and integrity of each component. On average, every open source package comes with 77 transitive dependencies; understanding OSS components and their dependencies is vital to any software company.

Static Application Security Testing (SAST).

Static Analysis is a vital and cost-effective tool to analyze source code to identify vulnerabilities early in the SDLC. SAST tooling is integrated into Cribl's code repository and integrated into software engineering IDEs. Cribl's Product Security Team writes customized SAST rules to ensure tailored coverage of Cribl's codebase, reduction of false positives, and increased detection of security antipatterns.

Dynamic Application Security Testing (DAST).

Dynamic Analysis tools analyze applications in their running state. This approach helps identify security flaws that only become apparent during a program's execution, such as those related to user authentication, session management, and data validation processes. Because ensuring the health and maximum coverage of DAST scans can be a time intensive process, Cribl partners with a best in class service provider to manage nightly DAST scans for Cribl products. A letter of attestation for the managed DAST service can be provided to customers at any time.

Vulnerability management.

Resolving vulnerabilities is a top priority for Cribl's engineering teams. Vulnerabilities in Cribl's products are tracked centrally and monitored and measured for SLA remediation compliance. Root cause analyses are performed on vulnerabilities by Cribl's Product Security team to document secure patterns that can be used to prevent similar vulnerabilities and add verification mechanisms such as customized SAST rules to provide continuously improving security testing feedback to Cribl's engineering teams.

Third-party penetration testing.

Penetration testing simulates cyber attacks under controlled conditions to identify potential vulnerabilities in a system. Periodic penetration testing is used at Cribl to validate the efficacy of our processes and controls implemented to build secure software. Cribl contracts a highly qualified third-party to conduct penetration testing against Cribl products multiple times a year. A letter of engagement from the most recent penetration test is available at any time to Cribl customers.

Responsible disclosure.

The Cribl product security team acknowledges the valuable role that honest, independent security researchers and bug reporters play in the overall security of connected systems. As a result, we encourage the responsible reporting of any vulnerability that may be present in our applications and services. Cribl is committed to working with security researchers to verify and address potential vulnerabilities that are reported to us. Security issues may be reported directly to Cribl's security team via Cribl's Vulnerability Disclosure Program at cribl.io/security.

Interested in learning more about security at Cribl? Please join us in the #security channel in the Cribl Community Slack Workspace. Please visit community.cribl.io to join. You can also reach out directly to the security team via email at security@cribl.io.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

WP-0020-EN-4-0724