HORTONWORKS, INC. 5470 GREAT AMERICA PKWY,
SANTA CLARA, CA 95054 • HORTONWORKS.COM

Hortonworks Platform Security Process

Platform security assurance processes at Hortonworks feature continuous process improvement and secure software development lifecycle and governance. Hortonworks Platform Security Process (HDPSEC) includes both proactive scans and testing during software development and release cycle as well as processes to manage and remediate any potential vulnerabilities that are reported by customers, partners or Apache communities from deployments. Hortonworks has built security vulnerability assessment and remediation into the development and release processes to provide its customers with best in class, enterprise grade, and secure platforms. By building security in as part of SDLC, Hortonworks enables customers to securely deploy and operate Hortonworks software platforms with the most common configuration options. Hortonworks R&D and field teams work closely with the Apache communities to ensure that discovered vulnerabilities or exploits are addressed within the community and fixes are made available through official releases from both the Apache projects as well as Hortonworks provided updates.

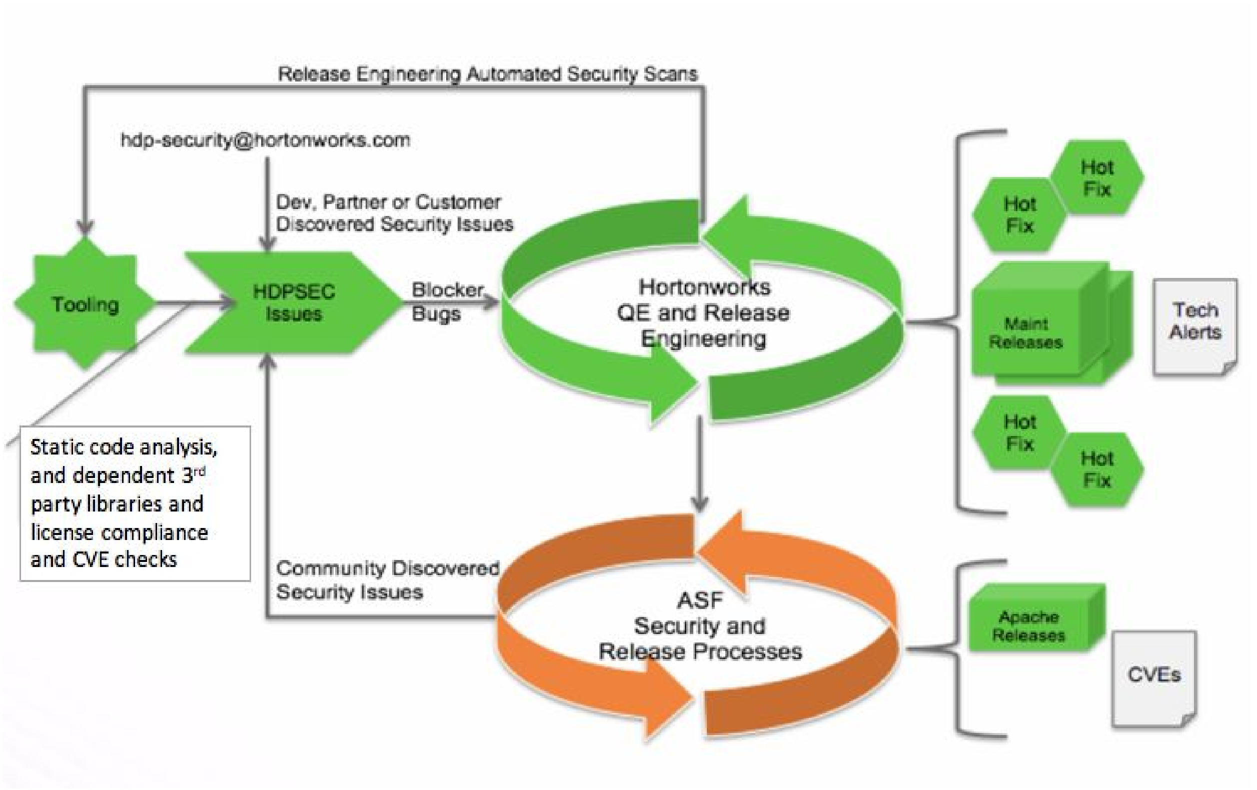
Note: Hortonworks does not share the results of static code scans or penetration testing with customers. This helps mitigate potential risks of exposure for our entire customer base, especially for the issues that were discovered internally, and are in the process of being addressed through the HDPSEC process.

Below are a few highlights of the HDPSEC process:

1. Hortonworks security experts monitor and track CVEs (Common Vulnerability and Exposures) via Apache CVE process and file appropriate security defects against specific components for prioritized remediation.
2. CVEs fixed in each release are added to release notes and made available to customers via the Hortonworks public documentation site. (as per Apache Security Process)
3. Technical Alerts are sent to customers when security fixes become available with detailed instructions to apply the relevant patch, upgrade, and/or maintenance release. *Note: There are times that a given release line is no longer supported, a hotfix introduces instability in a specific version, or the application of a hotfix is equivalent to upgrading to a later release. In such scenarios, Hortonworks may deem the most appropriate course of action to upgrade to a specific version instead of issuing a hotfix and will advise customers of the appropriate steps necessary.*
4. Scans to identify publicly reported vulnerabilities (CVEs) against dependent 3rd party libraries, as well as 3rd party license compliance checks are run during multiple stages in every product release.
5. Static scans are run on Apache project source code and release artifacts to identify any security vulnerabilities proactively and any critical vulnerabilities found are identified, tracked, and remediated in compliance with Apache security processes.

6. In addition, Hortonworks encourages customers to send an email to hdp-security@hortonworks.com for reporting any potential vulnerabilities or security issues. If Hortonworks security experts team determines that it needs to be addressed, HDPSEC process is initiated, and the issue is tracked through to resolution and customer delivery.

Below depicts the HDPSEC process:


Release Engineering Automated Security Scans
hdp-security@hortonworks.com
Dev, Partner or Customer Discovered Security Issues
Tooling
HDPSEC Issues
Blocker Bugs
Hortonworks QE and Release Engineering
Hot Fix
Hot Fix
Maint Releases
Tech Alerts
Hot Fix
Hot Fix
Static code analysis, and dependent 3rd party libraries and license compliance and CVE checks
Community Discovered Security Issues
ASF Security and Release Processes
Apache Releases
CVEs