



The Top 5 Open Source Vulnerabilities in Technology Companies

Leading Technology Organizations Automate Open Source Governance With the Nexus Platform



Organizations are Turning to Open Source

All organizations are turning to open source to speed time to innovation, but in technology companies, open source is at the forefront of their business. ISVs use open source to bring their products to market quickly and provide a competitive advantage, but with the benefit of speed comes some inherent risk.

In fact, 1 in 10 open source component download requests contain a known security vulnerability and the time from vulnerability identification to exploit has decreased from 45 days to 3 days within the last decade.¹ Also, according to a recent survey, 1 in 5 organizations suspected or verified a breach related to open source components.² In light of this and other security concerns, technology companies must rely on automated solutions to stay protected.

Software Vendors Need Automated Open Source Governance Solutions

With only 45% of organizations³ able to generate a software bill of materials, how do you prove that your product is safe? With automated open source governance solutions, you can shift security practices left and empower developers to select only the highest quality components. Generate a software bill of materials to identify all open source within an application to continuously manage risk and enforce open source policies across your entire software development lifecycle.



Create a Secure Development Environment: Enforce open source policies within the developer's IDE and SCM tools and quarantine bad components with an OSS firewall.



Provide Proof that Your Applications Are Secure: Automatically generate a software bill of materials (SBOM) to identify open source and third party libraries used within your software supply chain. SBOMs are quickly becoming a requirement from customers and potential acquirers during M&A due diligence.



Integrate Open Source Security Into Your DevOps Pipeline: Continuously monitor applications for new open source security risk and resolve quickly with expert remediation guidance.

“When we acquire a new company we will, as part of the due diligence, scan their products to make sure they don't have vulnerabilities that we are not prepared to accept. **[Nexus] helps us be sure that the target acquisition is of suitable quality in terms of its open-source use.**”

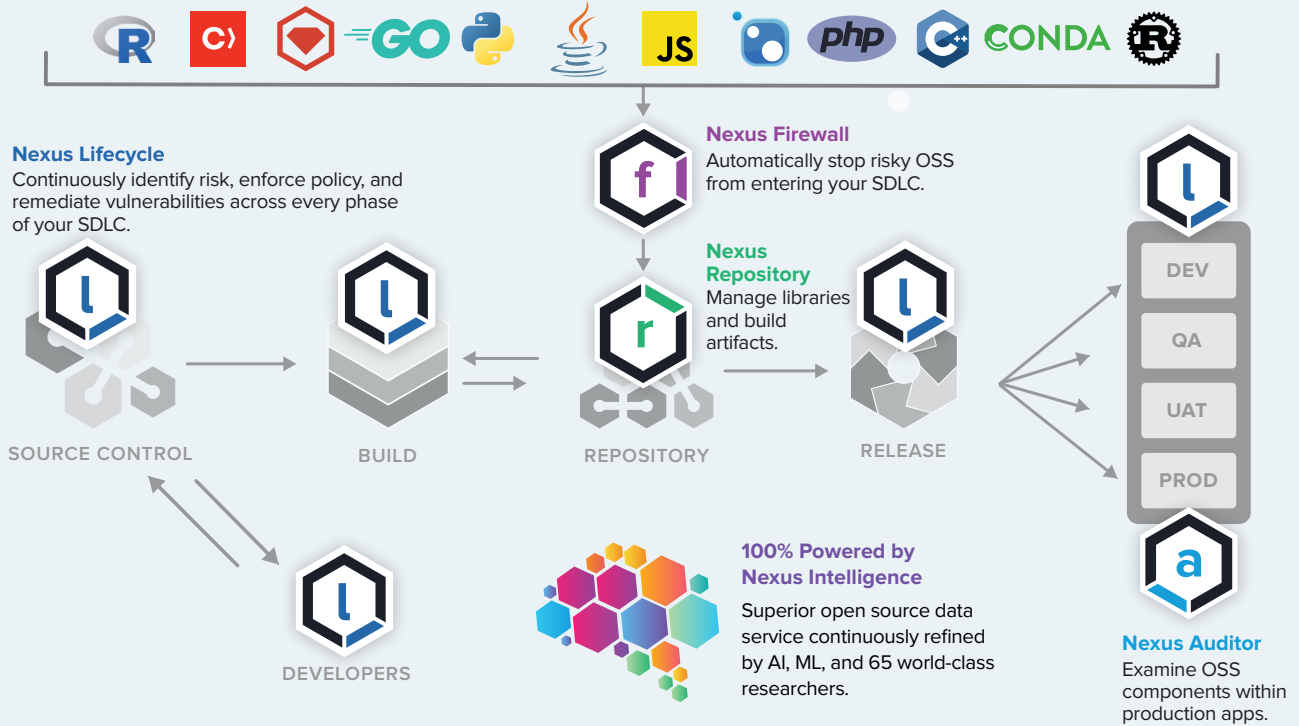
— A. COX, CIVICA, IT CENTRAL STATION REVIEW

¹ 2019 State of the Software Supply Chain Report, Sonatype

² 2020 DevSecOps Community Survey, Sonatype

³ 2020 DevSecOps Community Survey, Sonatype

Nexus automatically enforces open source policy and controls risk across every phase of the SDLC.



Precise component intelligence is a requirement to scale open source governance and create a secure software supply chain. With the Nexus Platform, technology companies have the deep insight they need to quickly identify and remediate security vulnerabilities. With more than 65 full time security researchers and over a decade of experience, we have identified...

The Top 5 Most Vulnerable Components Affecting Technology Companies Globally

Rank	Name	Component
5	Bouncycastle	org.bouncycastle:bcprov-jdk15on
4	lodash	lodash
3	Spring Framework	org.springframework:spring-web
2	Apache Tomcat	org.apache.tomcat.embed:tomcat-embed-core
1	Jackson Databind	com.fasterxml.jackson.core:jackson-databind

Number 5: Bouncycastle

Name of Vulnerability/Sonatype ID: CVE-2018-5382

Type of Vulnerability: Information Exposure

Severity: 9.8

CVSS 3.0 Metrics: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Components Affected:

- ▶ org.bouncycastle : bcprov-jdk14 : (, 1.47)
- ▶ org.bouncycastle : bcprov-jdk15on : (, 1.47)
- ▶ org.bouncycastle : bcprov-jdk16 : (,)

Remediation Recommendation: For users of `org.bouncycastle:bcprov-jdk14`` and `org.bouncycastle:bcprov-jdk15on`` components, upgrading to version 1.47 is the recommended solution. However, a fixed version for `org.bouncycastle:bcprov-jdk16`` component does not exist in Maven Central as of writing this piece.

In the fixed versions of Bouncycastle — i.e. 1.47 or newer, the BKS keystore format was updated to version 2, which uses a more rigorous HMAC of length 160-bit. This effectively resolves CVE-2018-5382.

“My advice is to use it as soon as you can. Implement it into your environment quickly because it’s going to help. **Your devs are going to thank you for it.”**

— W. KANAZAWA, PRIMERICA,
IT CENTRAL STATION REVIEW

Number 4: lodash

Type of Vulnerability: DoS, Remote code execution

Component Name: lodash (as present in npm)

Versions Affected: [4.17.5, 4.17.11)

Severity: 9.8

CVSS 3.0 Metrics: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Advisory Deviation: The Sonatype security research team discovered that the root cause of this vulnerability was introduced in version 4.17.5 due to an incomplete fix made for CVE-2018-3721. As a result, contrary to what the advisory states, only versions between 4.17.5 and 4.17.11 (exclusive) have been implicated for CVE-2018-16487. Vulnerable versions prior to 4.17.5 are still covered by CVE-2018-3721.

Remediation Recommendation: Users are recommended to upgrade to version 4.17.11 of `lodash`` which contains the fix. If upgrading is not a viable option, some developers have chosen to protect against this vulnerability by replacing a property entirely (rather than recursively extending it) if the destination object doesn’t have that property as its own. That would prevent traversing the built-in ‘constructor’ property, but wouldn’t prevent users from using the name ‘constructor’ in other contexts.



“Potential clients ask how we detect and address security issues. In our industry, a health system that houses patient information, **it is worthwhile to continuously monitor for security vulnerabilities and to address these concerns as soon as they come out.**”

— R. VAN DE BROEK, SOFTWARE ARCHITECT (TECH VENDOR), IT CENTRAL STATION REVIEW

Number 3: Spring Framework

Name of Vulnerability: CVE-2019-3773

Type of Vulnerability: XXE

Severity: 8.8

CVSS 3.0 Metrics: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Versions Affected:

- ▶ org.springframework.ws:spring-ws-core-tiger — All versions are vulnerable.
- ▶ org.springframework.ws:spring-xml:
 - ▶ For 3.x: all versions prior to 3.0.5.RELEASE are vulnerable.
 - ▶ For 1.x and 2.x: all versions prior to 2.4.4.RELEASE are vulnerable.
- ▶ org.springframework.ws:spring-ws-core:
 - ▶ For 3.x: all versions prior to 3.0.5.RELEASE are vulnerable.
 - ▶ For 1.x and 2.x: all versions prior to 2.4.4.RELEASE are vulnerable.

Remediation Recommendation: Luckily, the `TransformerFactoryUtils` and similar `*Utils` classes implemented in the fix for the vulnerability contains an in-built protection which prevents “external entities from accessing,” right when a `TransformerFactory` object is conceptualised. Therefore, when working with a project relying on XML data heavily, developers can incorporate the equivalent classes ending in `*Utils` to benefit from the inbuilt protections.

Sonatype recommends upgrading to version **3.0.5.RELEASE** or above of component `org.springframework.ws:spring-ws-core` which contains the fix for this vulnerability. For users of 1.x or 2.x, who are unable to upgrade to **3.0.5.RELEASE**, can upgrade to the fixed **2.4.4.RELEASE** instead.

Number 2: Apache Tomcat

Name of Vulnerability/Sonatype ID: CVE-2019-0232

Type of Vulnerability: Remote Code Execution

Apache Tomcat Versions Affected:

- ▶ org.apache.tomcat : tomcat-catalina : [9.0.0.M1, 9.0.19)
- ▶ org.apache.tomcat : tomcat-catalina : [8.0.0-RC1, 8.5.40)
- ▶ org.apache.tomcat : tomcat-catalina : [7.0.0, 7.0.94)
- ▶ org.apache.tomcat.embed : tomcat-embed-core : [9.0.0.M1, 9.0.19)
- ▶ org.apache.tomcat.embed : tomcat-embed-core : [8.0.0-RC1, 8.5.40)
- ▶ org.apache.tomcat.embed : tomcat-embed-core : [7.0.0, 7.0.94)

Remediation Recommendation:

The most obvious way to prevent a remote code execution attack with this specific vector is to upgrade to the appropriate version and to use proper development “hygiene” to avoid inadvertently enabling the *command line arguments* by altering the configuration. For 7.0.x, the advisory mentions upgrading to 7.0.93 which appears to be a typographical error as 7.0.93 is not a fixed version. Version 7.0.94 has been released and this contains the fix.

The fix incorporates “regex” pattern matching to prevent input from executing as commands on Windows systems.

Number 1 : Jackson Databind

Name of Vulnerability: Sonatype-2017-0312

Associated CVEs: CVE-2017-7525, CVE-2017-15095, CVE-2017-17485, CVE-2018-5968, CVE-2018-7489, CVE-2018-11307, CVE-2018-12022, CVE-2018-12023, CVE-2018-14718, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2019-12086, CVE-2019-12384, CVE-2019-12814, CVE-2019-14379, CVE-2019-14439, CVE-2019-14540, sonatype-2019-0371, and CVE-2019-16335.

Type of Vulnerability: Deserialization leading to Remote Code Execution (RCE)


Component Name: `com.fasterxml.jackson.core:jackson-databind`

Versions Affected: (, 2.10.0)

Criticality/CVSS Metrics: 8.5 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Recommendation:

As of today, we recommend upgrading to at least version 2.10.0 of `com.fasterxml.jackson.core:jackson-databind`, as present in Maven Central, and changing any usages of `enableDefaultTyping()` to `activateDefaultTyping()` in order to mitigate this vulnerability.



Are you currently using one of these vulnerable components? Can you quickly create a software bill of materials to find out?

DevOps-native organizations with the ability to continuously deploy software releases have an automation advantage that allows them to stay one step ahead of the hackers. Customers of Sonatype were notified of these vulnerabilities within hours of the discovery and their development teams automatically received instructions on how to remediate the risk.

Quickly determine if you are using one of these components by scanning your application with Sonatype's free [Nexus Vulnerability Scanner](#).



Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype's Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit [Sonatype.com](#), or connect with us on [Facebook](#), [Twitter](#), or [LinkedIn](#).

Headquarters

8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office

168 Shoreditch High St, 5th Fl
London E1 6JE
United Kingdom

APAC Office

5 Martin Place, Level 14
Sydney 2000, NSW
Australia

Sonatype Inc.

[www.sonatype.com](#)
Copyright 2020
All Rights Reserved.

