Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-43113
Title:	iTextPDF in iText 7 and up to (excluding 4.4.13.3) 7.1.17 allows comma ...
Package:	com.itextpdf:itextpdf
Package ID:	com.itextpdf:itextpdf:5.5.9
Installed Version:	5.5.9
Fixed Version:	5.5.13.3
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-77
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-43113
Description:	iTextPDF in iText 7 and up to (excluding 4.4.13.3) 7.1.17 allows command injecti on via a CompareTool filename that is mishandled on the gs (aka Ghostscript) com mand line in GhostscriptHelper.java.
References:	https://github.com/itext/itext7 https://github.com/itext/itext7/releases/tag/7.1 .17 https://github.com/itext/itextpdf/releases/tag/5.5.13.3 https://lists.debian .org/debian-lts-announce/2023/01/msg00013.html https://nvd.nist.gov/vuln/detail/ CVE-2021-43113 https://pastebin.com/BXnkY9YY https://www.debian.org/security/202 3/dsa-5323

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2015-7501
Title:	apache-commons-collections: InvokerTransformer code execution during deserialisation
Package:	commons-collections:commons-collections
Package ID:	commons-collections:commons-collections:3.2
Installed Version:	3.2
Fixed Version:	3.2.2
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2015-7501
Description:	Red Hat JBoss A-MQ 6.x; BPM Suite (BPMS) 6.x; BRMS 6.x and 5.x; Data Grid (JDG) 6.x; Data Virtualization (JDV) 6.x and 5.x; Enterprise Application Platform 6.x, 5.x, and 4.3.x; Fuse 6.x; Fuse Service Works (FSW) 6.x; Operations Network (JBoss ON) 3.x; Portal 6.x; SOA Platform (SOA-P) 5.x; Web Server (JWS) 3.x; Red Hat OpenShift/xPAAS 3.x; and Red Hat Subscription Asset Manager 1.3 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.

Vulnerability Report

References:	http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/ http://rhn.redha t.com/errata/RHSA-2015-2500.html http://rhn.redhat.com/errata/RHSA-2015-2501.htm l http://rhn.redhat.com/errata/RHSA-2015-2502.html http://rhn.redhat.com/errata/ RHSA-2015-2514.html http://rhn.redhat.com/errata/RHSA-2015-2516.html http://rhn. redhat.com/errata/RHSA-2015-2517.html http://rhn.redhat.com/errata/RHSA-2015-252 1.html http://rhn.redhat.com/errata/RHSA-2015-2522.html http://rhn.redhat.com/er

rata/RHSA-2015-2524.html
http://rhn.redhat.com/errata/RHSA-2015-2670.html
http:/
/rhn.redhat.com/errata/RHSA-2015-2671.html
http://rhn.redhat.com/errata/RHSA-201
6-0040.html
http://rhn.redhat.com/errata/RHSA-2016-1773.html
http://www.oracle.c
om/technetwork/security-advisory/cpuapr2018-3678067.html
http://www.oracle.com/t
echnetwork/security-advisory/cpujan2018-3236628.html
http://www.oracle.com/techn
etwork/security-advisory/cpujul2018-4258247.html
http://www.oracle.com/technetwo
rk/security-advisory/cpuoct2018-4428296.html
http://www.securityfocus.com/bid/78
215
http://www.securitytracker.com/id/1034097
http://www.securitytracker.com/id/
1037052
http://www.securitytracker.com/id/1037053
http://www.securitytracker.com
/id/1037640
https://access.redhat.com/security/cve/CVE-2015-7501
https://access.
redhat.com/security/vulnerabilities/2059393
https://access.redhat.com/solutions/
2045023
https://arxiv.org/pdf/2306.05534.pdf
https://bugzilla.redhat.com/show_bu
g.cgi?id=1279330
https://commons.apache.org/proper/commons-collections/release_4
_1.html
https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss
-jenkins-opennms-and-your-application-have-in-common-this-vulnerability
https://
github.com/apache/commons-collections

Vulnerability Report

https://github.com/jensdietrich/xshady-rel
ease/tree/main/CVE-2015-7501
https://issues.apache.org/jira/browse/COLLECTIONS-5
80.
https://linux.oracle.com/cve/CVE-2015-7501.html
https://linux.oracle.com/err
ata/ELSA-2015-2671.html
https://nvd.nist.gov/vuln/detail/CVE-2015-7501
https://r
hn.redhat.com/errata/RHSA-2015-2536.html
https://security.netapp.com/advisory/nt
ap-20240216-0010/
https://sourceforge.net/p/collections/code/HEAD/tree
https://w
ww.cve.org/CVERecord?id=CVE-2015-7501
https://www.oracle.com/security-alerts/cpu
jul2020.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2020-10683
Title:	dom4j: XML External Entity vulnerability in default SAX parser
Package:	dom4j:dom4j
Package ID:	dom4j:dom4j:1.1
Installed Version:	1.1
Fixed Version:	N/A
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-611
Primary URL:	https://avd.aquasec.com/nvd/cve-2020-10683
Description:	dom4j before 2.0.3 and 2.1.x before 2.1.3 allows external DTDs and External Enti ties by default, which might enable XXE attacks. However, there is popular exter nal documentation from OWASP showing how to enable the safe, non-default behavio r in any application that uses dom4j.

Vulnerability Report

References:	http://lists.opensuse.org/opensuse-security-announce/2020-05/msg00061.html https ://access.redhat.com/security/cve/CVE-2020-10683 https://bugzilla.redhat.com/sho w_bug.cgi?id=1694235 https://cheatsheetseries.owasp.org/cheatsheets/XML_External _Entity_Prevention_Cheat_Sheet.html https://github.com/dom4j/dom4j https://githu b.com/dom4j/dom4j/commit/1707bf3d898a8ada3b213acb0e3b38f16eaae73d https://github .com/dom4j/dom4j/commit/a8228522a99a02146106672a34c104adbda5c658 https://github. com/dom4j/dom4j/commits/version-2.0.3 https://github.com/dom4j/dom4j/issues/87 h ttps://github.com/dom4j/dom4j/releases/tag/version-2.1.3 https://lists.apache.or g/thread.html/r51f3f9801058e47153c0ad9bc6209d57a592fc0e7aefd787760911b8%40%3Cdev .velocity.apache.org%3E

Vulnerability Report

https://lists.apache.org/thread.html/r51f3f9801058e47153
c0ad9bc6209d57a592fc0e7aefd787760911b8@%3Cdev.velocity.apache.org%3E
https://lis
ts.apache.org/thread.html/r91c64cd51e68e97d524395474eaa25362d564572276b9917fcbf5
c32%40%3Cdev.velocity.apache.org%3E
https://lists.apache.org/thread.html/r91c64c
d51e68e97d524395474eaa25362d564572276b9917fcbf5c32@%3Cdev.velocity.apache.org%3E
https://lists.apache.org/thread.html/rb1b990d7920ae0d50da5109b73b92bab736d46c97
88dd4b135cb1a51%40%3Cnotifications.freemarker.apache.org%3E
https://lists.apache
.org/thread.html/rb1b990d7920ae0d50da5109b73b92bab736d46c9788dd4b135cb1a51@%3Cno
tifications.freemarker.apache.org%3E
https://nvd.nist.gov/vuln/detail/CVE-2020-1
0683
https://security.netapp.com/advisory/ntap-20200518-0002
https://security.ne
tapp.com/advisory/ntap-20200518-0002/
https://ubuntu.com/security/notices/USN-45
75-1
https://usn.ubuntu.com/4575-1
https://usn.ubuntu.com/4575-1/
https://www.cv
e.org/CVERecord?id=CVE-2020-10683
https://www.oracle.com//security-alerts/cpujul
2021.html
https://www.oracle.com/security-alerts/cpuApr2021.html
https://www.ora
cle.com/security-alerts/cpujan2021.html
https://www.oracle.com/security-alerts/c
pujan2022.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://ww
w.oracle.com/security-alerts/cpujul2022.html
https://www.oracle.com/security-ale
rts/cpuoct2020.html
https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2025-24813
Title:	tomcat: Potential RCE and/or information disclosure and/or information corruptio n with partial PUT
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.3, 10.1.35, 9.0.99
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-44, CWE-502, CWE-706
Primary URL:	https://avd.aquasec.com/nvd/cve-2025-24813

Vulnerability Report

Description:	Path Equivalence: 'file.Name' (Internal Dot) leading toÂ Remote Code Execution an d/or Information disclosureÂ and/or malicious content added to uploaded files via write enabledÂ Default ServletÂ in Apache Tomcat. This issue affects Apache Tomc at: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98. If all of the following were true, a malicious user was able t o view security sensitive files and/or inject content into those files: -Â writes enabled for the default servlet (disabled by default) - support for parti al PUT (enabled by default) - a target URL for security sensitive uploads that w as a sub-directory ofÂ a target URL for public uploads -Â attacker knowledge of th e names of security sensitive files beingÂ uploaded -Â the security sensitive file s also being uploaded via partial PUT If all of the following were true, a mali cious user was able to perform remote code execution:

Vulnerability Report

- writes enabled for
the default servlet (disabled by default)
-Â support for partial PUT (enabled by
default)
-Â application was using Tomcat's file based session persistence with t
heÂ default storage location
-Â application included a library that may be leverag
ed in aÂ deserialization attack
Users are recommended to upgrade to version 11.0
.3, 10.1.35 or 9.0.99, which fixes the issue.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2025/03/10/5 https://access.redhat.co m/errata/RHSA-2025:3645 https://access.redhat.com/security/cve/CVE-2025-24813 ht tps://bugzilla.redhat.com/2332817 https://bugzilla.redhat.com/2351129 https://er rata.almalinux.org/9/ALSA-2025-3645.html https://github.com/absholi7ly/POC-CVE-2 025-24813/blob/main/README.md https://github.com/apache/tomcat https://github.co m/apache/tomcat/commit/0a668e0c27f2b7ca0cc7c6eea32253b9b5ecb29c https://github.c om/apache/tomcat/commit/eb61aade8f8daccaecabf07d428b877975622f72 https://github. com/apache/tomcat/commit/f6c01d6577cf9a1e06792be47e623d36acc3b5dc https://linux. oracle.com/cve/CVE-2025-24813.html https://linux.oracle.com/errata/ELSA-2025-368 3.html https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq https:// lists.debian.org/debian-lts-announce/2025/04/msg00003.html https://nvd.nist.gov/

Vulnerability Report

vuln/detail/CVE-2025-24813
https://security.netapp.com/advisory/ntap-20250321-00
01
https://security.netapp.com/advisory/ntap-20250321-0001/
https://www.cisa.gov
/known-exploited-vulnerabilities-catalog
https://www.cve.org/CVERecord?id=CVE-20
25-24813
https://www.vicarius.io/vsociety/posts/cve-2025-24813-detect-apache-tom
cat-rce
https://www.vicarius.io/vsociety/posts/cve-2025-24813-mitigate-apache-to
mcat-rce

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-23926
Title:	xmlbeans: allowed malicious XML input may lead to XML Entity Expansion attack
Package:	org.apache.xmlbeans:xmlbeans
Package ID:	org.apache.xmlbeans:xmlbeans:2.6.0
Installed Version:	2.6.0
Fixed Version:	3.0.0
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.1
CWE:	CWE-776
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-23926
Description:	The XML parsers used by XMLBeans up to version 2.6.0 did not set the properties needed to protect the user from malicious XML input. Vulnerabilities include pos sibilities for XML Entity Expansion attacks. Affects XMLBeans up to and includin g v2.6.0.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2021-23926 https://issues.apache.org/ jira/browse/XMLBEANS-517 https://lists.apache.org/thread.html/r2dc5588009dc9f031 0b7382269f932cc96cae4c3901b747dda1a7fed%40%3Cjava-dev.axis.apache.org%3E https:/ /lists.apache.org/thread.html/r2dc5588009dc9f0310b7382269f932cc96cae4c3901b747dd a1a7fed@%3Cjava-dev.axis.apache.org%3E https://lists.apache.org/thread.html/rbb0 1d10512098894cd5f22325588197532c64f1c818ea7e4120d40c1%40%3Cjava-dev.axis.apache. org%3E https://lists.apache.org/thread.html/rbb01d10512098894cd5f22325588197532c 64f1c818ea7e4120d40c1@%3Cjava-dev.axis.apache.org%3E https://lists.debian.org/de bian-lts-announce/2021/06/msg00024.html https://nvd.nist.gov/vuln/detail/CVE-202 1-23926 https://poi.apache.org https://poi.apache.org/ https://security.netapp.c

Vulnerability Report

om/advisory/ntap-20210513-0004
https://security.netapp.com/advisory/ntap-2021051
3-0004/
https://www.cve.org/CVERecord?id=CVE-2021-23926
https://www.oracle.com/s
ecurity-alerts/cpujul2022.html
https://www.oracle.com/security-alerts/cpuoct2021
.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-20873
Title:	spring-boot: Security Bypass With Wildcard Pattern Matching on Cloud Foundry
Package:	org.springframework.boot:spring-boot-actuator-autoconfigure
Package ID:	org.springframework.boot:spring-boot-actuator-autoconfigure:2.6.2
Installed Version:	2.6.2
Fixed Version:	3.0.6, 2.7.11, 2.6.15, 2.5.15
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	N/A
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-20873
Description:	In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported ver sions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigat ion: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+ . Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2023-20873 https://github.com/advisor ies/GHSA-g5h3-w546-pj7f https://github.com/spring-projects/spring-boot https://g ithub.com/spring-projects/spring-boot/commit/32444fed4b51cc58dc908467f706102d7f0 bfc15 https://github.com/spring-projects/spring-boot/commit/3522714c13b47af03bf4 2e7f2d5994af568cb1a7 https://github.com/spring-projects/spring-boot/releases/tag /v2.5.15 https://github.com/spring-projects/spring-boot/releases/tag/v2.6.15 htt ps://github.com/spring-projects/spring-boot/releases/tag/v2.7.11 https://github. com/spring-projects/spring-boot/releases/tag/v3.0.6 https://nvd.nist.gov/vuln/de tail/CVE-2023-20873 https://security.netapp.com/advisory/ntap-20230601-0009

Vulnerability Report

http
s://security.netapp.com/advisory/ntap-20230601-0009/
https://spring.io/blog/2023
/05/18/spring-boot-2-5-15-and-2-6-15-available-now
https://spring.io/security/cv
e-2023-20873
https://spring.io/security/cve-2023-20873/
https://www.cve.org/CVER
ecord?id=CVE-2023-20873

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-22965
Title:	spring-framework: RCE via Data Binding on JDK 9+
Package:	org.springframework.boot:spring-boot-starter-web
Package ID:	org.springframework.boot:spring-boot-starter-web:2.6.2
Installed Version:	2.6.2
Fixed Version:	2.5.12, 2.6.6
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-94
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-22965
Description:	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

Vulnerability Report

References:	http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html htt p://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Pro perty-Remote-Code-Execution.html https://access.redhat.com/security/cve/CVE-2022 -22965 https://bugalert.org/content/notices/2022-03-30-spring.html https://cert- portal.siemens.com/productcert/pdf/ssa-254054.pdf https://github.com/spring-proj ects/spring-boot/releases/tag/v2.5.12 https://github.com/spring-projects/spring- boot/releases/tag/v2.6.6 https://github.com/spring-projects/spring-framework htt ps://github.com/spring-projects/spring-framework/commit/002546b3e4b8d791ea6acccb 81eb3168f51abb15 https://github.com/spring-projects/spring-framework/issues/2826

Vulnerability Report

0
https://github.com/spring-projects/spring-framework/releases/tag/v5.2.20.RELEA
SE
https://github.com/spring-projects/spring-framework/releases/tag/v5.3.18
http
s://nvd.nist.gov/vuln/detail/CVE-2022-22965
https://psirt.global.sonicwall.com/v
uln-detail/SNWLID-2022-0005
https://spring.io/blog/2022/03/31/spring-framework-r
ce-early-announcement
https://tanzu.vmware.com/security/cve-2022-22965
https://t
ools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-sprin
g-rce-Zx9GUc67
https://ubuntu.com/security/notices/USN-7165-1
https://www.cisa.g
ov/known-exploited-vulnerabilities-catalog
https://www.cve.org/CVERecord?id=CVE-
2022-22965
https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploit-
code.html
https://www.kb.cert.org/vuls/id/970766
https://www.oracle.com/security
-alerts/cpuapr2022.html
https://www.oracle.com/security-alerts/cpujul2022.html
h
ttps://www.praetorian.com/blog/spring-core-jdk9-rce/

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-22965
Title:	spring-framework: RCE via Data Binding on JDK 9+
Package:	org.springframework:spring-beans
Package ID:	org.springframework:spring-beans:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.2.20.RELEASE, 5.3.18
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-94
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-22965
Description:	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

Vulnerability Report

References:	http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html htt p://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Pro perty-Remote-Code-Execution.html https://access.redhat.com/security/cve/CVE-2022 -22965 https://bugalert.org/content/notices/2022-03-30-spring.html https://cert- portal.siemens.com/productcert/pdf/ssa-254054.pdf https://github.com/spring-proj ects/spring-boot/releases/tag/v2.5.12 https://github.com/spring-projects/spring- boot/releases/tag/v2.6.6 https://github.com/spring-projects/spring-framework htt ps://github.com/spring-projects/spring-framework/commit/002546b3e4b8d791ea6acccb 81eb3168f51abb15 https://github.com/spring-projects/spring-framework/issues/2826

Vulnerability Report

0
https://github.com/spring-projects/spring-framework/releases/tag/v5.2.20.RELEA
SE
https://github.com/spring-projects/spring-framework/releases/tag/v5.3.18
http
s://nvd.nist.gov/vuln/detail/CVE-2022-22965
https://psirt.global.sonicwall.com/v
uln-detail/SNWLID-2022-0005
https://spring.io/blog/2022/03/31/spring-framework-r
ce-early-announcement
https://tanzu.vmware.com/security/cve-2022-22965
https://t
ools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-sprin
g-rce-Zx9GUc67
https://ubuntu.com/security/notices/USN-7165-1
https://www.cisa.g
ov/known-exploited-vulnerabilities-catalog
https://www.cve.org/CVERecord?id=CVE-
2022-22965
https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploit-
code.html
https://www.kb.cert.org/vuls/id/970766
https://www.oracle.com/security
-alerts/cpuapr2022.html
https://www.oracle.com/security-alerts/cpujul2022.html
h
ttps://www.praetorian.com/blog/spring-core-jdk9-rce/

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2016-1000027
Title:	spring: HttpInvokerServiceExporter readRemoteInvocation method untrusted java de serialization
Package:	org.springframework:spring-web
Package ID:	org.springframework:spring-web:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.0.0
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2016-1000027
Description:	Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2016-1000027 https://bugzilla.redhat. com/show_bug.cgi?id=CVE-2016-1000027 https://github.com/spring-projects/spring-f ramework https://github.com/spring-projects/spring-framework/commit/2b051b8b3217 68a4cfef83077db65c6328ffd60f https://github.com/spring-projects/spring-framework /commit/5cbe90b2cd91b866a5a9586e460f311860e11cfa https://github.com/spring-proje cts/spring-framework/issues/21680 https://github.com/spring-projects/spring-fram ework/issues/24434 https://github.com/spring-projects/spring-framework/issues/24 434#issuecomment-1231625331 https://github.com/spring-projects/spring-framework/ issues/24434#issuecomment-579669626

Vulnerability Report

https://github.com/spring-projects/spring-fr
amework/issues/24434#issuecomment-582313417
https://github.com/spring-projects/s
pring-framework/issues/24434#issuecomment-744519525
https://jira.spring.io/brows
e/SPR-17143?redirect=false
https://nvd.nist.gov/vuln/detail/CVE-2016-1000027
htt
ps://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/100
0xxx/CVE-2016-1000027.json
https://security-tracker.debian.org/tracker/CVE-2016-
1000027
https://security.netapp.com/advisory/ntap-20230420-0009
https://security
.netapp.com/advisory/ntap-20230420-0009/
https://spring.io/blog/2022/05/11/sprin
g-framework-5-3-20-and-5-2-22-available-now
https://support.contrastsecurity.com
/hc/en-us/articles/4402400830612-Spring-web-Java-Deserialization-CVE-2016-100002
7
https://www.cve.org/CVERecord?id=CVE-2016-1000027
https://www.tenable.com/secu
rity/research/tra-2016-20

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-22965
Title:	spring-framework: RCE via Data Binding on JDK 9+
Package:	org.springframework:spring-webmvc
Package ID:	org.springframework:spring-webmvc:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.2.20.RELEASE, 5.3.18
Source:	ghsa
Severity:	CRITICAL
CVSS Score:	9.8
CWE:	CWE-94
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-22965
Description:	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

Vulnerability Report

References:	http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html htt p://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Pro perty-Remote-Code-Execution.html https://access.redhat.com/security/cve/CVE-2022 -22965 https://bugalert.org/content/notices/2022-03-30-spring.html https://cert- portal.siemens.com/productcert/pdf/ssa-254054.pdf https://github.com/spring-proj ects/spring-boot/releases/tag/v2.5.12 https://github.com/spring-projects/spring- boot/releases/tag/v2.6.6 https://github.com/spring-projects/spring-framework htt ps://github.com/spring-projects/spring-framework/commit/002546b3e4b8d791ea6acccb 81eb3168f51abb15 https://github.com/spring-projects/spring-framework/issues/2826

Vulnerability Report

0
https://github.com/spring-projects/spring-framework/releases/tag/v5.2.20.RELEA
SE
https://github.com/spring-projects/spring-framework/releases/tag/v5.3.18
http
s://nvd.nist.gov/vuln/detail/CVE-2022-22965
https://psirt.global.sonicwall.com/v
uln-detail/SNWLID-2022-0005
https://spring.io/blog/2022/03/31/spring-framework-r
ce-early-announcement
https://tanzu.vmware.com/security/cve-2022-22965
https://t
ools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-sprin
g-rce-Zx9GUc67
https://ubuntu.com/security/notices/USN-7165-1
https://www.cisa.g
ov/known-exploited-vulnerabilities-catalog
https://www.cve.org/CVERecord?id=CVE-
2022-22965
https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploit-
code.html
https://www.kb.cert.org/vuls/id/970766
https://www.oracle.com/security
-alerts/cpuapr2022.html
https://www.oracle.com/security-alerts/cpujul2022.html
h
ttps://www.praetorian.com/blog/spring-core-jdk9-rce/

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-6378
Title:	logback: serialization vulnerability in logback receiver
Package:	ch.qos.logback:logback-classic
Package ID:	ch.qos.logback:logback-classic:1.2.9
Installed Version:	1.2.9
Fixed Version:	1.3.12, 1.4.12, 1.2.13
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.1
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-6378
Description:	A serialization vulnerability in logback receiver component part of logback ver sion 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending p oisoned data.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2023-6378 https://github.com/qos-ch/l ogback https://github.com/qos-ch/logback/commit/9c782b45be4abdafb7e17481e24e7354 c2acd1eb https://github.com/qos-ch/logback/commit/b8eac23a9de9e05fb6d51160b3f46a cd91af9731 https://github.com/qos-ch/logback/commit/bb095154be011267b64e37a1d401 546e7cc2b7c3 https://github.com/qos-ch/logback/issues/745#issuecomment-183622715 8 https://logback.qos.ch/manual/receivers.html https://logback.qos.ch/news.html# 1.2.13 https://logback.qos.ch/news.html#1.3.12 https://nvd.nist.gov/vuln/detail/ CVE-2023-6378

Vulnerability Report

https://security.netapp.com/advisory/ntap-20241129-0012
https://se
curity.netapp.com/advisory/ntap-20241129-0012/
https://www.cve.org/CVERecord?id=
CVE-2023-6378

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-6378
Title:	logback: serialization vulnerability in logback receiver
Package:	ch.qos.logback:logback-core
Package ID:	ch.qos.logback:logback-core:1.2.9
Installed Version:	1.2.9
Fixed Version:	1.3.12, 1.4.12, 1.2.13
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.1
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-6378
Description:	A serialization vulnerability in logback receiver component part of logback ver sion 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending p oisoned data.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2023-6378 https://github.com/qos-ch/l ogback https://github.com/qos-ch/logback/commit/9c782b45be4abdafb7e17481e24e7354 c2acd1eb https://github.com/qos-ch/logback/commit/b8eac23a9de9e05fb6d51160b3f46a cd91af9731 https://github.com/qos-ch/logback/commit/bb095154be011267b64e37a1d401 546e7cc2b7c3 https://github.com/qos-ch/logback/issues/745#issuecomment-183622715 8 https://logback.qos.ch/manual/receivers.html https://logback.qos.ch/news.html# 1.2.13 https://logback.qos.ch/news.html#1.3.12 https://nvd.nist.gov/vuln/detail/ CVE-2023-6378

Vulnerability Report

https://security.netapp.com/advisory/ntap-20241129-0012
https://se
curity.netapp.com/advisory/ntap-20241129-0012/
https://www.cve.org/CVERecord?id=
CVE-2023-6378

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2020-36518
Title:	jackson-databind: denial of service via a large depth of nested objects
Package:	com.fasterxml.jackson.core:jackson-databind
Package ID:	com.fasterxml.jackson.core:jackson-databind:2.13.1
Installed Version:	2.13.1
Fixed Version:	2.13.2.1, 2.12.6.1
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-787
Primary URL:	https://avd.aquasec.com/nvd/cve-2020-36518
Description:	jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.

Vulnerability Report

References:	https://access.redhat.com/errata/RHSA-2023:2312 https://access.redhat.com/securi ty/cve/CVE-2020-36518 https://bugzilla.redhat.com/2064698 https://errata.almalin ux.org/9/ALSA-2023-2312.html https://github.com/FasterXML/jackson-databind https ://github.com/FasterXML/jackson-databind/commit/0a8157c6ca478b1bc7be4ba7dccdb386 3275f0de https://github.com/FasterXML/jackson-databind/commit/3cc52f82ecf943e06c 1d7c3b078e405fb3923d2b https://github.com/FasterXML/jackson-databind/commit/8238 ab41d0350fb915797c89d46777b4496b74fd https://github.com/FasterXML/jackson-databi nd/commit/b3587924ee5d8695942f364d0d404d48d0ea6126 https://github.com/FasterXML/ jackson-databind/commit/fcfc4998ec23f0b1f7f8a9521c2b317b6c25892b https://github. com/FasterXML/jackson-databind/issues/2816 https://github.com/FasterXML/jackson/ wiki/Jackson-Release-2.12

Vulnerability Report

https://github.com/FasterXML/jackson/wiki/Jackson-Rele
ase-2.13
https://github.com/advisories/GHSA-57j2-w4cx-62h2
https://linux.oracle.
com/cve/CVE-2020-36518.html
https://linux.oracle.com/errata/ELSA-2024-3061.html
https://lists.debian.org/debian-lts-announce/2022/05/msg00001.html
https://lists
.debian.org/debian-lts-announce/2022/11/msg00035.html
https://nvd.nist.gov/vuln/
detail/CVE-2020-36518
https://security.netapp.com/advisory/ntap-20220506-0004
ht
tps://security.netapp.com/advisory/ntap-20220506-0004/
https://www.cve.org/CVERe
cord?id=CVE-2020-36518
https://www.debian.org/security/2022/dsa-5283
https://www
.oracle.com/security-alerts/cpuapr2022.html
https://www.oracle.com/security-aler
ts/cpujul2022.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-42003
Title:	jackson-databind: deep wrapper array nesting wrt UNWRAP_SINGLE_VALUE_ARRAYS
Package:	com.fasterxml.jackson.core:jackson-databind
Package ID:	com.fasterxml.jackson.core:jackson-databind:2.13.1
Installed Version:	2.13.1
Fixed Version:	2.12.7.1, 2.13.4.2
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-42003
Description:	In FasterXML jackson-databind before versions 2.13.4.1 and 2.12.17.1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2022-42003 https://bugs.chromium.org/ p/oss-fuzz/issues/detail?id=51020 https://github.com/FasterXML/jackson-databind https://github.com/FasterXML/jackson-databind/blob/2.13/release-notes/VERSION-2. x https://github.com/FasterXML/jackson-databind/commit/0e37a39502439ecbaa1a5b518 8387c01bf7f7fa1 https://github.com/FasterXML/jackson-databind/commit/2c4a601c626 f7790cad9d3c322d244e182838288 https://github.com/FasterXML/jackson-databind/comm it/7ba9ac5b87a9d6ac0d2815158ecbeb315ad4dcdc https://github.com/FasterXML/jackson -databind/commit/cd090979b7ea78c75e4de8a4aed04f7e9fa8deea https://github.com/Fas terXML/jackson-databind/commit/d499f2e7bbc5ebd63af11e1f5cf1989fa323aa45 https:// github.com/FasterXML/jackson-databind/commit/d78d00ee7b5245b93103fef3187f70543d6 7ca33

Vulnerability Report

https://github.com/FasterXML/jackson-databind/commit/d78d00ee7b5245b93103f
ef3187f70543d67ca33 (jackson-databind-2.14.0-rc1)
https://github.com/FasterXML/j
ackson-databind/commits/jackson-databind-2.4.0-rc1?after=75b97b8519f0d50c62523ad
85170d80a197a2c86+174&branch=jackson-databind-2.4.0-rc1&qualified_name=refs%2Fta
gs%2Fjackson-databind-2.4.0-rc1
https://github.com/FasterXML/jackson-databind/co
mpare/jackson-databind-2.13.4.1...jackson-databind-2.13.4.2
https://github.com/F
asterXML/jackson-databind/issues/3590
https://github.com/FasterXML/jackson-datab
ind/issues/3627
https://lists.debian.org/debian-lts-announce/2022/11/msg00035.ht
ml
https://nvd.nist.gov/vuln/detail/CVE-2022-42003
https://security.gentoo.org/g
lsa/202210-21
https://security.netapp.com/advisory/ntap-20221124-0004
https://se
curity.netapp.com/advisory/ntap-20221124-0004/
https://www.cve.org/CVERecord?id=
CVE-2022-42003
https://www.debian.org/security/2022/dsa-5283

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-42004
Title:	jackson-databind: use of deeply nested arrays
Package:	com.fasterxml.jackson.core:jackson-databind
Package ID:	com.fasterxml.jackson.core:jackson-databind:2.13.1
Installed Version:	2.13.1
Fixed Version:	2.12.7.1, 2.13.4
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-42004
Description:	In FasterXML jackson-databind before 2.13.4, resource exhaustion can occur because of a lack of a check in BeanDeserializer._deserializeFromArray to prevent use of deeply nested arrays. An application is vulnerable only with certain customized choices for deserialization.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2022-42004 https://bugs.chromium.org/ p/oss-fuzz/issues/detail?id=50490 https://github.com/FasterXML/jackson-databind https://github.com/FasterXML/jackson-databind/commit/063183589218fec19a9293ed2f1 7ec53ea80ba88 https://github.com/FasterXML/jackson-databind/commit/063183589218f ec19a9293ed2f17ec53ea80ba88 (jackson-databind-2.13.4) https://github.com/FasterX ML/jackson-databind/commit/35de19e7144c4df8ab178b800ba86e80c3d84252 https://gith ub.com/FasterXML/jackson-databind/commit/cd090979b7ea78c75e4de8a4aed04f7e9fa8dee a https://github.com/FasterXML/jackson-databind/issues/3582 https://lists.debian .org/debian-lts-announce/2022/11/msg00035.html https://nvd.nist.gov/vuln/detail/ CVE-2022-42004 https://security.gentoo.org/glsa/202210-21

Vulnerability Report

https://security.netap
p.com/advisory/ntap-20221118-0008
https://security.netapp.com/advisory/ntap-2022
1118-0008/
https://www.cve.org/CVERecord?id=CVE-2022-42004
https://www.debian.or
g/security/2022/dsa-5283

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-25647
Title:	com.google.code.gson-gson: Deserialization of Untrusted Data in com.google.code.gson-gson
Package:	com.google.code.gson:gson
Package ID:	com.google.code.gson:gson:2.8.6
Installed Version:	2.8.6
Fixed Version:	2.8.9
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.7
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-25647
Description:	The package com.google.code.gson:gson before 2.8.9 are vulnerable to Deserialization of Untrusted Data via the writeReplace() method in internal classes, which may lead to DoS attacks.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2022-25647 https://github.com/google/ gson https://github.com/google/gson/pull/1991 https://github.com/google/gson/pul l/1991/commits https://linux.oracle.com/cve/CVE-2022-25647.html https://linux.or acle.com/errata/ELSA-2022-9656.html https://lists.debian.org/debian-lts-announce /2022/05/msg00015.html https://lists.debian.org/debian-lts-announce/2022/09/msg0 0009.html https://nvd.nist.gov/vuln/detail/CVE-2022-25647 https://security.netap p.com/advisory/ntap-20220901-0009 https://security.netapp.com/advisory/ntap-2022 0901-0009/ https://snyk.io/vuln/SNYK-JAVA-COMGOOGLECODEGSON-1730327 https://ubun

Vulnerability Report

tu.com/security/notices/USN-6692-1
https://www.cve.org/CVERecord?id=CVE-2022-256
47
https://www.debian.org/security/2022/dsa-5227
https://www.oracle.com/security
-alerts/cpujul2022.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2017-9096
Title:	itext: External entities not disabled
Package:	com.itextpdf:itextpdf
Package ID:	com.itextpdf:itextpdf:5.5.9
Installed Version:	5.5.9
Fixed Version:	5.5.12, 7.0.3
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.8
CWE:	CWE-611
Primary URL:	https://avd.aquasec.com/nvd/cve-2017-9096
Description:	The XML parsers in iText before 5.5.12 and 7.x before 7.0.3 do not disable exter nal entities, which might allow remote attackers to conduct XML external entity (XXE) attacks via a crafted PDF.
References:	http://www.securityfocus.com/archive/1/541483/100/0/threaded https://access.redh at.com/security/cve/CVE-2017-9096 https://nvd.nist.gov/vuln/detail/CVE-2017-9096 https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hp esbhf03902en_us https://www.compass-security.com/fileadmin/Datein/Research/Advis ories/CSNC-2017-017_itext_xml_external_entity_attack.txt https://www.cve.org/CVE Record?id=CVE-2017-9096 https://www.oracle.com/security-alerts/cpuoct2020.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2019-10086
Title:	apache-commons-beanutils: does not suppresses the class property in PropertyUtil sBean by default
Package:	commons-beanutils:commons-beanutils
Package ID:	commons-beanutils:commons-beanutils:1.7.0
Installed Version:	1.7.0
Fixed Version:	1.9.4
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.3
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2019-10086
Description:	In Apache Commons Beanutils 1.9.2, a special BeanIntrospector class was added wh ich allows suppressing the ability for an attacker to access the classloader via the class property available on all Java objects. We, however were not using th is by default characteristic of the PropertyUtilsBean.

Vulnerability Report

http://lists.opensuse.org/opensuse-security-announce/2019-09/msg00007.html

http:

//mail-archives.apache.org/mod_mbox/www-announce/201908.mbox/%3cC628798F-315D-44

28-8CB1-4ED1ECC958E4%40apache.org%3e

http://mail-archives.apache.org/mod_mbox/ww

w-announce/201908.mbox/%3cC628798F-315D-4428-8CB1-4ED1ECC958E4@apache.org%3e

htt

ps://access.redhat.com/errata/RHSA-2019:4317

https://access.redhat.com/errata/RH

SA-2020:0057

https://access.redhat.com/errata/RHSA-2020:0194

https://access.redh

at.com/errata/RHSA-2020:0804

https://access.redhat.com/errata/RHSA-2020:0805

htt

ps://access.redhat.com/errata/RHSA-2020:0806

https://access.redhat.com/errata/RH

SA-2020:0811

https://access.redhat.com/security/cve/CVE-2019-10086

Vulnerability Report

https://commo
ns.apache.org/proper/commons-beanutils/javadocs/v1.9.4/RELEASE-NOTES.txt
https:/
/github.com/apache/commons-beanutils
https://github.com/apache/commons-beanutils
/commit/dd48f4e589462a8cdb1f29bbbccb35d6b0291d58
https://github.com/apache/commo
ns-beanutils/pull/7
https://issues.apache.org/jira/browse/BEANUTILS-520
https://
linux.oracle.com/cve/CVE-2019-10086.html
https://linux.oracle.com/errata/ELSA-20
20-0194.html
https://lists.apache.org/thread.html/02094ad226dbc17a2368beaf27e61d
8b1432f5baf77d0ca995bb78bc%40%3Cissues.commons.apache.org%3E
https://lists.apach
e.org/thread.html/02094ad226dbc17a2368beaf27e61d8b1432f5baf77d0ca995bb78bc@%3Cis
sues.commons.apache.org%3E
https://lists.apache.org/thread.html/1f78f1e32cc5614e
c0c5b822ba4bd7fc8e8b5c46c8e038b6bd609cb5%40%3Cissues.commons.apache.org%3E
https
://lists.apache.org/thread.html/1f78f1e32cc5614ec0c5b822ba4bd7fc8e8b5c46c8e038b6
bd609cb5@%3Cissues.commons.apache.org%3E
https://lists.apache.org/thread.html/2f
d61dc89df9aeab738d2b49f48d42c76f7d53b980ba04e1d48bce48%40%3Cdev.shiro.apache.org
%3E
https://lists.apache.org/thread.html/2fd61dc89df9aeab738d2b49f48d42c76f7d53b
980ba04e1d48bce48@%3Cdev.shiro.apache.org%3E
https://lists.apache.org/thread.htm
l/3d1ed1a1596c08c4d5fea97b36c651ce167b773f1afc75251ce7a125%40%3Ccommits.tinkerpo
p.apache.org%3E
https://lists.apache.org/thread.html/3d1ed1a1596c08c4d5fea97b36c
651ce167b773f1afc75251ce7a125@%3Ccommits.tinkerpop.apache.org%3E
https://lists.a
pache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f%4
0%3Cdev.drill.apache.org%3E
https://lists.apache.org/thread.html/519eb0fd45642dc

Vulnerability Report

ecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E
https://lis
ts.apache.org/thread.html/5261066cd7adee081ee05c8bf0e96cf0b2eeaced391e19117ae4da
a6%40%3Cdev.shiro.apache.org%3E
https://lists.apache.org/thread.html/5261066cd7a
dee081ee05c8bf0e96cf0b2eeaced391e19117ae4daa6@%3Cdev.shiro.apache.org%3E
https:/
/lists.apache.org/thread.html/956995acee0d8bc046f1df0a55b7fbeb65dd2f82864e5de107
8bacb0%40%3Cissues.commons.apache.org%3E
https://lists.apache.org/thread.html/95
6995acee0d8bc046f1df0a55b7fbeb65dd2f82864e5de1078bacb0@%3Cissues.commons.apache.
org%3E
https://lists.apache.org/thread.html/a684107d3a78e431cf0fbb90629e8559a36f
f8fe94c3a76e620b39fa%40%3Cdev.shiro.apache.org%3E
https://lists.apache.org/threa
d.html/a684107d3a78e431cf0fbb90629e8559a36ff8fe94c3a76e620b39fa@%3Cdev.shiro.apa
che.org%3E
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca668
02ef9a2a12ee199f5b0c1442%40%3Cdev.drill.apache.org%3E
https://lists.apache.org/t
hread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill
.apache.org%3E
https://lists.apache.org/thread.html/c94bc9649d5109a663b2129371dc
45753fbdeacd340105548bbe93c3%40%3Cdev.shiro.apache.org%3E
https://lists.apache.o
rg/thread.html/c94bc9649d5109a663b2129371dc45753fbdeacd340105548bbe93c3@%3Cdev.s
hiro.apache.org%3E
https://lists.apache.org/thread.html/d6ca9439c53374b597f33b7e
c180001625597db48ea30356af01145f%40%3Cdev.shiro.apache.org%3E
https://lists.apac
he.org/thread.html/d6ca9439c53374b597f33b7ec180001625597db48ea30356af01145f@%3Cd
ev.shiro.apache.org%3E
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a
69aae6d53e609a758e34d2869b4d798e13cc%40%3Cissues.drill.apache.org%3E
https://lis
ts.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13
cc@%3Cissues.drill.apache.org%3E

Vulnerability Report

https://lists.apache.org/thread.html/r18d8b4f92
63e5cad3bbaef0cdba0e2ccdf9201316ac4b85e23eb7ee4%40%3Cdev.atlas.apache.org%3E
htt
ps://lists.apache.org/thread.html/r18d8b4f9263e5cad3bbaef0cdba0e2ccdf9201316ac4b
85e23eb7ee4@%3Cdev.atlas.apache.org%3E
https://lists.apache.org/thread.html/r2d5
f1d88c39bd615271abda63964a0bee9b2b57fef1f84cb4c43032e%40%3Cissues.nifi.apache.or
g%3E
https://lists.apache.org/thread.html/r2d5f1d88c39bd615271abda63964a0bee9b2b
57fef1f84cb4c43032e@%3Cissues.nifi.apache.org%3E
https://lists.apache.org/thread
.html/r306c0322aa5c0da731e03f3ce9f07f4745c052c6b73f4e78faf232ca%40%3Cdev.atlas.a
pache.org%3E
https://lists.apache.org/thread.html/r306c0322aa5c0da731e03f3ce9f07
f4745c052c6b73f4e78faf232ca@%3Cdev.atlas.apache.org%3E
https://lists.apache.org/
thread.html/r43de02fd4a4f52c4bdeff8c02f09625d83cd047498009c1cdab857db%40%3Cdev.r
ocketmq.apache.org%3E
https://lists.apache.org/thread.html/r43de02fd4a4f52c4bdef
f8c02f09625d83cd047498009c1cdab857db@%3Cdev.rocketmq.apache.org%3E
https://lists
.apache.org/thread.html/r46e536fc98942dce99fadd2e313aeefe90c1a769c5cd85d98df9d09
8%40%3Cissues.nifi.apache.org%3E
https://lists.apache.org/thread.html/r46e536fc9
8942dce99fadd2e313aeefe90c1a769c5cd85d98df9d098@%3Cissues.nifi.apache.org%3E
htt
ps://lists.apache.org/thread.html/r513a7a21c422170318115463b399dd58ab447fe0990b1
3e5884f0825%40%3Ccommits.dolphinscheduler.apache.org%3E
https://lists.apache.org
/thread.html/r513a7a21c422170318115463b399dd58ab447fe0990b13e5884f0825@%3Ccommit
s.dolphinscheduler.apache.org%3E
https://lists.apache.org/thread.html/r6194ced48
28deb32023cd314e31f41c61d388b58935d102c7de91f58%40%3Cdev.atlas.apache.org%3E
htt
ps://lists.apache.org/thread.html/r6194ced4828deb32023cd314e31f41c61d388b58935d1
02c7de91f58@%3Cdev.atlas.apache.org%3E
https://lists.apache.org/thread.html/r967

Vulnerability Report

953a14e05016bc4bcae9ef3dd92e770181158b4246976ed8295c9%40%3Cdev.brooklyn.apache.o
rg%3E
https://lists.apache.org/thread.html/r967953a14e05016bc4bcae9ef3dd92e77018
1158b4246976ed8295c9@%3Cdev.brooklyn.apache.org%3E
https://lists.apache.org/thre
ad.html/ra41fd0ad4b7e1d675c03a5081a16a6603085a4e37d30b866067566fe%40%3Cissues.ni
fi.apache.org%3E
https://lists.apache.org/thread.html/ra41fd0ad4b7e1d675c03a5081
a16a6603085a4e37d30b866067566fe@%3Cissues.nifi.apache.org%3E
https://lists.apach
e.org/thread.html/ra87ac17410a62e813cba901fdd4e9a674dd53daaf714870f28e905f1%40%3
Cdev.atlas.apache.org%3E
https://lists.apache.org/thread.html/ra87ac17410a62e813
cba901fdd4e9a674dd53daaf714870f28e905f1@%3Cdev.atlas.apache.org%3E
https://lists
.apache.org/thread.html/ra9a139fdc0999750dcd519e81384bc1fe3946f311b1796221205f51
c%40%3Ccommits.dolphinscheduler.apache.org%3E
https://lists.apache.org/thread.ht
ml/ra9a139fdc0999750dcd519e81384bc1fe3946f311b1796221205f51c@%3Ccommits.dolphins
cheduler.apache.org%3E
https://lists.apache.org/thread.html/racd3e7b2149fa2f255f
016bd6bffab0fea77b6fb81c50db9a17f78e6%40%3Cdev.atlas.apache.org%3E
https://lists
.apache.org/thread.html/racd3e7b2149fa2f255f016bd6bffab0fea77b6fb81c50db9a17f78e
6@%3Cdev.atlas.apache.org%3E
https://lists.apache.org/thread.html/rae81e0c8ebdf4
7ffaa85a01240836bfece8a990c48f55c7933162b5c%40%3Cdev.atlas.apache.org%3E
https:/
/lists.apache.org/thread.html/rae81e0c8ebdf47ffaa85a01240836bfece8a990c48f55c793
3162b5c@%3Cdev.atlas.apache.org%3E
https://lists.apache.org/thread.html/rb1f76c2
c0a4d6efb8a3523974f9d085d5838b73e7bffdf9a8f212997%40%3Cissues.nifi.apache.org%3E
https://lists.apache.org/thread.html/rb1f76c2c0a4d6efb8a3523974f9d085d5838b73e7
bffdf9a8f212997@%3Cissues.nifi.apache.org%3E
https://lists.apache.org/thread.htm
l/rb8dac04cb7e9cc5dedee8dabaa1c92614f590642e5ebf02a145915ba%40%3Ccommits.atlas.a

pache.org%3E
https://lists.apache.org/thread.html/rb8dac04cb7e9cc5dedee8dabaa1c9
2614f590642e5ebf02a145915ba@%3Ccommits.atlas.apache.org%3E
https://lists.apache.
org/thread.html/rcc029be4edaaf5b8bb85818aab494e16f312fced07a0f4a202771ba2%40%3Ci
ssues.nifi.apache.org%3E
https://lists.apache.org/thread.html/rcc029be4edaaf5b8b
b85818aab494e16f312fced07a0f4a202771ba2@%3Cissues.nifi.apache.org%3E
https://lis
ts.apache.org/thread.html/rd2d2493f4f1af6980d265b8d84c857e2b7ab80a46e1423710c448
957%40%3Cissues.nifi.apache.org%3E
https://lists.apache.org/thread.html/rd2d2493
f4f1af6980d265b8d84c857e2b7ab80a46e1423710c448957@%3Cissues.nifi.apache.org%3E
h
ttps://lists.apache.org/thread.html/re2028d4d76ba1db3e3c3a722d6c6034e801cc3b309f
69cc166eaa32b%40%3Ccommits.nifi.apache.org%3E
https://lists.apache.org/thread.ht
ml/re2028d4d76ba1db3e3c3a722d6c6034e801cc3b309f69cc166eaa32b@%3Ccommits.nifi.apa
che.org%3E
https://lists.apache.org/thread.html/re3cd7cb641d7fc6684e4fc3c336a8ba
d4a01434bb5625a06e3600fd1%40%3Cissues.nifi.apache.org%3E
https://lists.apache.or
g/thread.html/re3cd7cb641d7fc6684e4fc3c336a8bad4a01434bb5625a06e3600fd1@%3Cissue
s.nifi.apache.org%3E
https://lists.apache.org/thread.html/rec74f3a94dd850259c730
b4ba6f7b6211222b58900ec088754aa0534%40%3Cissues.nifi.apache.org%3E
https://lists
.apache.org/thread.html/rec74f3a94dd850259c730b4ba6f7b6211222b58900ec088754aa053
4@%3Cissues.nifi.apache.org%3E
https://lists.apache.org/thread.html/reee57101464
cf7622d640ae013b2162eb864f603ec4093de8240bb8f%40%3Cdev.atlas.apache.org%3E
https
://lists.apache.org/thread.html/reee57101464cf7622d640ae013b2162eb864f603ec4093d
e8240bb8f@%3Cdev.atlas.apache.org%3E
https://lists.debian.org/debian-lts-announc
e/2019/08/msg00030.html
https://lists.fedoraproject.org/archives/list/package-an

nounce%40lists.fedoraproject.org/message/4APPGLBWMFAS4WHNLR4LIJ65DJGPV7TF/
https
://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.
org/message/JIUYSL2RSIWZVNSUIXJTIFPIPIF6OAIO/
https://lists.fedoraproject.org/ar
chives/list/package-announce@lists.fedoraproject.org/message/4APPGLBWMFAS4WHNLR4
LIJ65DJGPV7TF
https://lists.fedoraproject.org/archives/list/package-announce@lis
ts.fedoraproject.org/message/JIUYSL2RSIWZVNSUIXJTIFPIPIF6OAIO
https://nvd.nist.g
ov/vuln/detail/CVE-2019-10086
https://ubuntu.com/security/notices/USN-4766-1
htt
ps://www.cve.org/CVERecord?id=CVE-2019-10086
https://www.oracle.com//security-al
erts/cpujul2021.html
https://www.oracle.com/security-alerts/cpuApr2021.html
http
s://www.oracle.com/security-alerts/cpuapr2020.html
https://www.oracle.com/securi
ty-alerts/cpuapr2022.html
https://www.oracle.com/security-alerts/cpujan2020.html
https://www.oracle.com/security-alerts/cpujan2021.html
https://www.oracle.com/s
ecurity-alerts/cpujan2022.html
https://www.oracle.com/security-alerts/cpujul2020
.html
https://www.oracle.com/security-alerts/cpujul2022.html
https://www.oracle.
com/security-alerts/cpuoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2015-6420
Title:	Insecure Deserialization in Apache Commons Collection
Package:	commons-collections:commons-collections
Package ID:	commons-collections:commons-collections:3.2
Installed Version:	3.2
Fixed Version:	3.2.2
Source:	ghsa
Severity:	HIGH
CVSS Score:	N/A
CWE:	CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2015-6420
Description:	Serialized-object interfaces in certain Cisco Collaboration and Social Media; En dpoint Clients and Client Software; Network Application, Service, and Accelerati on; Network and Content Security Devices; Network Management and Provisioning; R outing and Switching - Enterprise and Service Provider; Unified Computing; Voice and Unified Communications Devices; Video, Streaming, TelePresence, and Transco ding Devices; Wireless; and Cisco Hosted Services products allow remote attacker s to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.

Vulnerability Report

References:	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20 151209-java-deserialization http://www.oracle.com/technetwork/security-advisory/ cpujul2018-4258247.html http://www.securityfocus.com/bid/78872 https://arxiv.org /pdf/2306.05534 https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphe re-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/ https://github.com/apache/commons-collections https://h20566.www2.hpe.com/porta l/site/hpsc/public/kb/docDisplay?docId=emr_na-c05376917 https://h20566.www2.hpe. com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722 https://lists.a

Vulnerability Report

pache.org/thread.html/r352e40ca9874d1beb4ad95403792adca7eb295e6bc3bd7b65fabcc21%
40%3Ccommits.samza.apache.org%3E
https://lists.apache.org/thread.html/r352e40ca9
874d1beb4ad95403792adca7eb295e6bc3bd7b65fabcc21@%3Ccommits.samza.apache.org%3E
h
ttps://news.apache.org/foundation/entry/apache_commons_statement_to_widespread
h
ttps://nvd.nist.gov/vuln/detail/CVE-2015-6420
https://www.kb.cert.org/vuls/id/57
6313
https://www.kb.cert.org/vuls/id/581311
https://www.tenable.com/security/res
earch/tra-2017-14
https://www.tenable.com/security/research/tra-2017-23

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-47554
Title:	apache-commons-io: Possible denial of service attack on untrusted input to XmlStreamReader
Package:	commons-io:commons-io
Package ID:	commons-io:commons-io:2.3
Installed Version:	2.3
Fixed Version:	2.14.0
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-400
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-47554
Description:	Uncontrolled Resource Consumption vulnerability in Apache Commons IO. The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input. This issue affects Apache Commons IO: from 2.0 before 2.14.0. Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.

Vulnerability Report

References:

http://www.openwall.com/lists/oss-security/2024/10/03/2

https://access.redhat.co

m/security/cve/CVE-2024-47554

https://github.com/apache/commons-io

https://lists

.apache.org/thread/6ozr91rr9cj5lm0zyhv30bsp317hk5z1

https://nvd.nist.gov/vuln/de

tail/CVE-2024-47554

https://security.netapp.com/advisory/ntap-20250131-0010

http

s://security.netapp.com/advisory/ntap-20250131-0010/

Vulnerability Report

https://www.cve.org/CVEReco
rd?id=CVE-2024-47554

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2018-1000632
Title:	dom4j: XML Injection in Class: Element. Methods: addElement, addAttribute which can impact the integrity of XML documents
Package:	dom4j:dom4j
Package ID:	dom4j:dom4j:1.1
Installed Version:	1.1
Fixed Version:	N/A
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-91
Primary URL:	https://avd.aquasec.com/nvd/cve-2018-1000632
Description:	dom4j version prior to version 2.1.1 contains a CWE-91: XML Injection vulnerability in Class: Element. Methods: addElement, addAttribute that can result in an attacker tampering with XML documents through XML injection. This attack appear to be exploitable via an attacker specifying attributes or elements in the XML document. This vulnerability appears to have been fixed in 2.1.1 or later.

Vulnerability Report

https://access.redhat.com/errata/RHSA-2019:0362

https://access.redhat.com/errata

/RHSA-2019:0364

https://access.redhat.com/errata/RHSA-2019:0365

https://access.r

edhat.com/errata/RHSA-2019:0380

https://access.redhat.com/errata/RHSA-2019:1159

https://access.redhat.com/errata/RHSA-2019:1160

https://access.redhat.com/errata

/RHSA-2019:1161

https://access.redhat.com/errata/RHSA-2019:1162

https://access.r

edhat.com/errata/RHSA-2019:3172

https://access.redhat.com/security/cve/CVE-2018-

1000632

https://github.com/advisories/GHSA-6pcc-3rfx-4gpm

https://github.com/dom

Vulnerability Report

4j/dom4j
https://github.com/dom4j/dom4j/commit/c2a99d7dee8ce7a4e5bef134bb781a667
2bd8a0f
https://github.com/dom4j/dom4j/commit/e598eb43d418744c4dbf62f647dd2381c9
ce9387
https://github.com/dom4j/dom4j/issues/48
https://ihacktoprotect.com/post/
dom4j-xml-injection
https://ihacktoprotect.com/post/dom4j-xml-injection/
https:/
/lists.apache.org/thread.html/00571f362a7a2470fba50a31282c65637c40d2e21ebe6ee535
a4ed74%40%3Ccommits.maven.apache.org%3E
https://lists.apache.org/thread.html/005
71f362a7a2470fba50a31282c65637c40d2e21ebe6ee535a4ed74@%3Ccommits.maven.apache.or
g%3E
https://lists.apache.org/thread.html/4a77652531d62299a30815cf5f233af183425d
b8e3c9a824a814e768%40%3Cdev.maven.apache.org%3E
https://lists.apache.org/thread.
html/4a77652531d62299a30815cf5f233af183425db8e3c9a824a814e768@%3Cdev.maven.apach
e.org%3E
https://lists.apache.org/thread.html/5a020ecaa3c701f408f612f7ba2ee37a02
1644c4a39da2079ed3ddbc%40%3Ccommits.maven.apache.org%3E
https://lists.apache.org
/thread.html/5a020ecaa3c701f408f612f7ba2ee37a021644c4a39da2079ed3ddbc@%3Ccommits
.maven.apache.org%3E
https://lists.apache.org/thread.html/708d94141126eac0301114
4a971a6411fcac16d9c248d1d535a39451%40%3Csolr-user.lucene.apache.org%3E
https://l
ists.apache.org/thread.html/708d94141126eac03011144a971a6411fcac16d9c248d1d535a3
9451@%3Csolr-user.lucene.apache.org%3E
https://lists.apache.org/thread.html/7e9e
78f0e4288fac6591992836d2a80d4df19161e54bd71ab4b8e458%40%3Cdev.maven.apache.org%3
E
https://lists.apache.org/thread.html/7e9e78f0e4288fac6591992836d2a80d4df19161e
54bd71ab4b8e458@%3Cdev.maven.apache.org%3E
https://lists.apache.org/thread.html/
7f6e120e6ed473f4e00dde4c398fc6698eb383bd7857d20513e989ce%40%3Cdev.maven.apache.o

rg%3E
https://lists.apache.org/thread.html/7f6e120e6ed473f4e00dde4c398fc6698eb38
3bd7857d20513e989ce@%3Cdev.maven.apache.org%3E
https://lists.apache.org/thread.h
tml/9d4c1af6f702c3d6d6f229de57112ddccac8ce44446a01b7937ab9e0%40%3Ccommits.maven.
apache.org%3E
https://lists.apache.org/thread.html/9d4c1af6f702c3d6d6f229de57112
ddccac8ce44446a01b7937ab9e0@%3Ccommits.maven.apache.org%3E
https://lists.apache.
org/thread.html/d7d960b2778e35ec9b4d40c8efd468c7ce7163bcf6489b633491c89f%40%3Cde
v.maven.apache.org%3E
https://lists.apache.org/thread.html/d7d960b2778e35ec9b4d4
0c8efd468c7ce7163bcf6489b633491c89f@%3Cdev.maven.apache.org%3E
https://lists.apa
che.org/thread.html/rb1b990d7920ae0d50da5109b73b92bab736d46c9788dd4b135cb1a51%40
%3Cnotifications.freemarker.apache.org%3E
https://lists.apache.org/thread.html/r
b1b990d7920ae0d50da5109b73b92bab736d46c9788dd4b135cb1a51@%3Cnotifications.freema
rker.apache.org%3E
https://lists.debian.org/debian-lts-announce/2018/09/msg00028
.html
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fed
oraproject.org/message/IOOVVCRQE6ATFD2JM2EMDXOQXTRIVZGP/
https://lists.fedorapro
ject.org/archives/list/package-announce%40lists.fedoraproject.org/message/KJULAH
VR3I5SX7OSMXAG75IMNSAYOXGA/
https://lists.fedoraproject.org/archives/list/packag
e-announce@lists.fedoraproject.org/message/IOOVVCRQE6ATFD2JM2EMDXOQXTRIVZGP
http
s://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.o
rg/message/KJULAHVR3I5SX7OSMXAG75IMNSAYOXGA
https://nvd.nist.gov/vuln/detail/CVE
-2018-1000632
https://security.netapp.com/advisory/ntap-20190530-0001
https://se
curity.netapp.com/advisory/ntap-20190530-0001/
https://ubuntu.com/security/notic

Vulnerability Report

es/USN-4619-1
https://www.cve.org/CVERecord?id=CVE-2018-1000632
https://www.orac
le.com/security-alerts/cpuApr2021.html
https://www.oracle.com/security-alerts/cp
uapr2020.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://www
.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2017-12626
Title:	poi: Parsing of multiple file types can cause a denial of service via infinite l oop or out of memory exception
Package:	org.apache.poi:poi
Package ID:	org.apache.poi:poi:3.13
Installed Version:	3.13
Fixed Version:	3.17
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-835
Primary URL:	https://avd.aquasec.com/nvd/cve-2017-12626
Description:	Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1) Infinite Loops while parsing crafted WMF, EMF, MSG and macros (POI bugs 61338 and 61294), and 2) Out of Memory Exceptions while parsing crafted DOC , PPT and XLS (POI bugs 52372 and 61295).

Vulnerability Report

References:	http://www.securityfocus.com/bid/102879 https://access.redhat.com/errata/RHSA-20 18:1322 https://access.redhat.com/security/cve/CVE-2017-12626 https://github.com /apache/poi https://lists.apache.org/thread.html/453d9af5dbabaccd9afb58d27279a9d bfe8e35f4e5ea1645ddd6960b%40%3Cdev.poi.apache.org%3E https://lists.apache.org/th read.html/453d9af5dbabaccd9afb58d27279a9dbfe8e35f4e5ea1645ddd6960b@%3Cdev.poi.ap ache.org%3E https://lists.apache.org/thread.html/708d94141126eac03011144a971a641 1fcac16d9c248d1d535a39451%40%3Csolr-user.lucene.apache.org%3E https://lists.apac he.org/thread.html/708d94141126eac03011144a971a6411fcac16d9c248d1d535a39451@%3Cs olr-user.lucene.apache.org%3E https://nvd.nist.gov/vuln/detail/CVE-2017-12626 ht tps://www.cve.org/CVERecord?id=CVE-2017-12626

Vulnerability Report

https://www.oracle.com/security-al
erts/cpuApr2021.html
https://www.oracle.com/security-alerts/cpuapr2020.html
http
s://www.oracle.com/security-alerts/cpujan2020.html
https://www.oracle.com/securi
ty-alerts/cpujan2021.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.oracle.com/security-alerts/cpuoct2020.html
https://www.oracle.com/t
echnetwork/security-advisory/cpuoct2019-5072832.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2015-0899
Title:	1: input validation bypass in MultiPageValidator
Package:	org.apache.struts:struts-core
Package ID:	org.apache.struts:struts-core:1.3.8
Installed Version:	1.3.8
Fixed Version:	N/A
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-20
Primary URL:	https://avd.aquasec.com/nvd/cve-2015-0899
Description:	The MultiPageValidator implementation in Apache Struts 1 1.1 through 1.3.10 allo ws remote attackers to bypass intended access restrictions via a modified page p arameter.

Vulnerability Report

References:	http://en.sourceforge.jp/projects/terasoluna/wiki/StrutsPatch2-EN http://jvn.jp/ en/jp/JVN86448949/index.html http://jvndb.jvn.jp/en/contents/2015/JVNDB-2015-000 042.html http://jvndb.jvn.jp/jvndb/JVNDB-2015-000042 http://www.debian.org/secur ity/2016/dsa-3536 http://www.oracle.com/technetwork/security-advisory/cpuoct2017 -3236626.html http://www.securityfocus.com/bid/74423 https://access.redhat.com/s ecurity/cve/CVE-2015-0899 https://en.osdn.jp/projects/terasoluna/wiki/StrutsPatc h2-EN https://jvn.jp/en/jp/JVN86448949/index.html https://nvd.nist.gov/vuln/deta il/CVE-2015-0899 https://security.netapp.com/advisory/ntap-20180629-0006 https:/ /security.netapp.com/advisory/ntap-20180629-0006/

Vulnerability Report

https://www.cve.org/CVERecord?
id=CVE-2015-0899

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2016-1181
Title:	struts: Vulnerability in ActionForm allows unintended remote operations against components on server memory
Package:	org.apache.struts:struts-core
Package ID:	org.apache.struts:struts-core:1.3.8
Installed Version:	1.3.8
Fixed Version:	N/A
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.1
CWE:	N/A
Primary URL:	https://avd.aquasec.com/nvd/cve-2016-1181
Description:	ActionServlet.java in Apache Struts 1 1.x through 1.3.10 mishandles multithreaded access to an ActionForm instance, which allows remote attackers to execute arbitrary code or cause a denial of service (unexpected memory access) via a multipart request, a related issue to CVE-2015-0899.

Vulnerability Report

References:	http://jvn.jp/en/jp/JVN03188560/index.html http://jvndb.jvn.jp/jvndb/JVNDB-2016- 000096 http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.ht ml http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html h ttp://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html http: //www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html http://ww w.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html http://www.or acle.com/technetwork/security-advisory/cpuoct2017-3236626.html http://www.oracle .com/technetwork/security-advisory/cpuoct2018-4428296.html http://www.securityfo cus.com/bid/91068 http://www.securityfocus.com/bid/91787

Vulnerability Report

http://www.securitytrac
ker.com/id/1036056
https://access.redhat.com/security/cve/CVE-2016-1181
https://
bugzilla.redhat.com/show_bug.cgi?id=1343538
https://github.com/kawasima/struts1-
forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8
https://jvn.jp/en/jp/JVN
03188560/
https://nvd.nist.gov/vuln/detail/CVE-2016-1181
https://security-tracke
r.debian.org/tracker/CVE-2016-1181
https://security.netapp.com/advisory/ntap-201
80629-0006
https://security.netapp.com/advisory/ntap-20180629-0006/
https://www.
cve.org/CVERecord?id=CVE-2016-1181
https://www.oracle.com/security-alerts/cpujan
2020.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.ora
cle.com/technetwork/security-advisory/cpuapr2019-5072813.html
https://www.oracle
.com/technetwork/security-advisory/cpujan2019-5072801.html
https://www.oracle.co
m/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2016-1182
Title:	struts: Improper input validation in Validator
Package:	org.apache.struts:struts-core
Package ID:	org.apache.struts:struts-core:1.3.8
Installed Version:	1.3.8
Fixed Version:	N/A
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.2
CWE:	CWE-20
Primary URL:	https://avd.aquasec.com/nvd/cve-2016-1182
Description:	ActionServlet.java in Apache Struts 1 1.x through 1.3.10 does not properly restr ict the Validator configuration, which allows remote attackers to conduct cross- site scripting (XSS) attacks or cause a denial of service via crafted input, a r elated issue to CVE-2015-0899.

Vulnerability Report

References:	http://jvn.jp/en/jp/JVN65044642/index.html http://jvndb.jvn.jp/jvndb/JVNDB-2016- 000097 http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.ht ml http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html h ttp://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html http: //www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html http://ww w.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html http://www.or acle.com/technetwork/security-advisory/cpuoct2018-4428296.html http://www.securi tyfocus.com/bid/91067 http://www.securityfocus.com/bid/91787 http://www.security tracker.com/id/1036056 https://access.redhat.com/security/cve/CVE-2016-1182

Vulnerability Report

http
s://bugzilla.redhat.com/show_bug.cgi?id=1343540
https://github.com/kawasima/stru
ts1-forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8
https://jvn.jp/en/jp
/JVN65044642/
https://nvd.nist.gov/vuln/detail/CVE-2016-1182
https://security-tr
acker.debian.org/tracker/CVE-2016-1182
https://security.netapp.com/advisory/ntap
-20180629-0006
https://security.netapp.com/advisory/ntap-20180629-0006/
https://
www.cve.org/CVERecord?id=CVE-2016-1182
https://www.oracle.com/security-alerts/cp
ujan2020.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://www
.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
https://www.or
acle.com/technetwork/security-advisory/cpujan2019-5072801.html
https://www.oracl
e.com/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-42252
Title:	tomcat: request smuggling
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	8.5.83, 9.0.68, 10.0.27, 10.1.1
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-444
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-42252
Description:	If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10 .1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting reje ctIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a r equest containing an invalid Content-Length header making a request smuggling at tack possible if Tomcat was located behind a reverse proxy that also failed to r eject the request with the invalid header.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2022-42252 https://github.com/apache/ tomcat https://github.com/apache/tomcat/commit/0d089a15047faf9cb3c82f80f4d28febd 4798920 https://github.com/apache/tomcat/commit/4c7f4fd09d2cc1692112ef70b8ee23a7 a037ae77 https://github.com/apache/tomcat/commit/4c7f4fd09d2cc1692112ef70b8ee23a 7a037ae77 (9.0.68) https://github.com/apache/tomcat/commit/a1c07906d8dcaf7957e5c c97f5cdbac7d18a205a https://github.com/apache/tomcat/commit/a1c07906d8dcaf7957e5 cc97f5cdbac7d18a205a (8.5.83) https://github.com/apache/tomcat/commit/c9fe754e5d 17e262dfbd3eab2a03ca96ff372dc3 https://lists.apache.org/thread/zzcxzvqfdqn515zfs 3dxb7n8gty589sq https://nvd.nist.gov/vuln/detail/CVE-2022-42252

Vulnerability Report

https://security
.gentoo.org/glsa/202305-37
https://tomcat.apache.org/security-10.html
https://to
mcat.apache.org/security-8.html
https://tomcat.apache.org/security-9.html
https:
//ubuntu.com/security/notices/USN-6880-1
https://www.cve.org/CVERecord?id=CVE-20
22-42252

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-45143
Title:	tomcat: JsonErrorReportValve injection
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	8.5.84, 9.0.69, 10.1.2
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-116
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-45143
Description:	The JsonErrorReportValve in Apache Tomcat 8.5.83, 9.0.40 to 9.0.68 and 10.1.0-M1 to 10.1.1 did not escape the type, message or description values. In some circumstances these are constructed from user provided data and it was therefore possible for users to supply values that invalidated or manipulated the JSON output.
References:	https://access.redhat.com/security/cve/CVE-2022-45143 https://github.com/apache/ tomcat https://github.com/apache/tomcat/commit/0cab3a56bd89f70e7481bb0d68395dc7e 130dbbf https://github.com/apache/tomcat/commit/6a0ac6a438cbbb66b6e9c5223842f53b f0cb50aa https://github.com/apache/tomcat/commit/b336f4e58893ea35114f1e4a415657f 723b1298e https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj https ://nvd.nist.gov/vuln/detail/CVE-2022-45143 https://security.gentoo.org/glsa/2023 05-37 https://security.netapp.com/advisory/ntap-20230216-0009/ https://www.cve.o rg/CVERecord?id=CVE-2022-45143

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-24998
Title:	FileUpload: FileUpload DoS with excessive parts
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	10.1.5, 11.0.0-M5, 8.5.88, 9.0.71
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-770
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-24998
Description:	Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS wit h a malicious upload or series of uploads. Note that, like all of the file u pload limits, the new configuration option (FileUploadBase#setFileCoun tMax) is not enabled by default and must be explicitly configured.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2023/05/22/1 https://access.redhat.co m/errata/RHSA-2023:6570 https://access.redhat.com/security/cve/CVE-2023-24998 ht tps://bugzilla.redhat.com/2172298 https://bugzilla.redhat.com/2180856 https://bu gzilla.redhat.com/2210321 https://commons.apache.org/proper/commons-fileupload/s ecurity-reports.html https://commons.apache.org/proper/commons-fileupload/securi

ty-reports.html#Fixed_in_Apache_Commons_FileUpload_1.5
https://errata.almalinux.
org/9/ALSA-2023-6570.html
https://github.com/apache/commons-fileupload
https://g
ithub.com/apache/commons-fileupload/commit/e20c04990f7420ca917e96a84cec58b13a1b3
d17
https://github.com/apache/tomcat/commit/8a2285f13affa961cc65595aad999db5efae
45ce
https://github.com/apache/tomcat/commit/9ca96c8c1eba86c0aaa2e6be581ba2a7d4d
4ae6e
https://github.com/apache/tomcat/commit/cf77cc545de0488fb89e24294151504a74
32df74
https://github.com/apache/tomcat/commit/d53d8e7f77042cc32a3b98f589496a1ef
5088e38
https://github.com/search?q=repo%3Aapache%2Ftomcat+util.http+path%3A%2F%
5Eres%5C%2Fbnd%5C%2F%2F&type=code
https://linux.oracle.com/cve/CVE-2023-24998.ht
ml
https://linux.oracle.com/errata/ELSA-2023-7065.html
https://lists.apache.org/
thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy
https://lists.debian.org/debian-lts-anno
unce/2023/10/msg00020.html
https://nvd.nist.gov/vuln/detail/CVE-2023-24998
https
://security.gentoo.org/glsa/202305-37
https://security.netapp.com/advisory/ntap-
20230302-0013
https://security.netapp.com/advisory/ntap-20230302-0013/
https://t
omcat.apache.org/security-10.html
https://tomcat.apache.org/security-11.html
htt
ps://tomcat.apache.org/security-8.html
https://tomcat.apache.org/security-9.html

Vulnerability Report

https://www.cve.org/CVERecord?id=CVE-2023-24998
https://www.debian.org/security
/2023/dsa-5522

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-46589
Title:	tomcat: HTTP request smuggling via malformed trailer headers
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.0-M11, 10.1.16, 9.0.83, 8.5.96
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-444
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-46589
Description:	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 t hrough 11.0.0-M10, from 10.1.0-M1 through 10.1.15, from 9.0.0-M1 through 9.0.82 and from 8.5.0 through 8.5.95 did not correctly parse HTTP trailer headers. A tr ailer header that exceeded the header size limit could cause Tomcat to treat a s ingle request as multiple requests leading to the possibility of request smugg ling when behind a reverse proxy. Users are recommended to upgrade to version 1 1.0.0-M11Â onwards, 10.1.16 onwards, 9.0.83 onwards or 8.5.96 onwards, which fix the issue.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2023/11/28/2 https://access.redhat.co m/errata/RHSA-2024:1134 https://access.redhat.com/security/cve/CVE-2023-46589 ht tps://bugzilla.redhat.com/2252050 https://bugzilla.redhat.com/show_bug.cgi?id=22 52050 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46589 https://erra ta.almalinux.org/9/ALSA-2024-1134.html https://errata.rockylinux.org/RLSA-2024:0

Vulnerability Report

539
https://github.com/apache/tomcat
https://github.com/apache/tomcat/commit/0a1
1905b67fdff58f4efa77fb099ca9967a709b3 (8.5.64)
https://github.com/apache/tomcat/
commit/6f181e1062a472bc5f0234980f66cbde42c1041b
https://github.com/apache/tomcat
/commit/7a2d8818fcea0b51747a67af9510ce7977245ebd
https://github.com/apache/tomca
t/commit/7a2d8818fcea0b51747a67af9510ce7977245ebd (9.0.83)
https://github.com/ap
ache/tomcat/commit/aa92971e879a519384c517febc39fd04c48d4642
https://github.com/a
pache/tomcat/commit/aa92971e879a519384c517febc39fd04c48d4642 (8.5.96)
https://gi
thub.com/apache/tomcat/commit/abdf1d8e8a8f12d1956f2828bf22b9846a6dcdef (8.5.96)
https://github.com/apache/tomcat/commit/b5776d769bffeade865061bc8ecbeb2b56167b08
https://github.com/apache/tomcat/commit/b5776d769bffeade865061bc8ecbeb2b56167b0
8 (10.1.16)
https://github.com/apache/tomcat/commit/bcacd783e2593ae9b2c07a561bd5
f95a145a7761 (8.5.40)
https://linux.oracle.com/cve/CVE-2023-46589.html
https://l
inux.oracle.com/errata/ELSA-2024-1134.html
https://lists.apache.org/thread/0rqq6
ktozqc42ro8hhxdmmdjm1k1tpxr
https://lists.debian.org/debian-lts-announce/2024/01
/msg00001.html
https://nvd.nist.gov/vuln/detail/CVE-2023-46589
https://security.
netapp.com/advisory/ntap-20231214-0009
https://security.netapp.com/advisory/ntap
-20231214-0009/
https://tomcat.apache.org/security-10.html
https://tomcat.apache

Vulnerability Report

.org/security-11.html
https://tomcat.apache.org/security-8.html
https://tomcat.a
pache.org/security-9.html
https://ubuntu.com/security/notices/USN-7032-1
https:/
/www.cve.org/CVERecord?id=CVE-2023-46589
https://www.openwall.com/lists/oss-secu
rity/2023/11/28/2

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-34750
Title:	tomcat: Improper Handling of Exceptional Conditions
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.0-M21, 10.1.25, 9.0.90
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-400, CWE-755
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-34750
Description:	Improper Handling of Exceptional Conditions, Uncontrolled Resource Consumption vulnerability in Apache Tomcat. When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.0-M1 through 9.0.89. Users are recommended to upgrade to version 11.0.0-M21, 10.1.25 or 9.0.90, which fixes the issue.

Vulnerability Report

References:	https://access.redhat.com/errata/RHSA-2024:5693 https://access.redhat.com/securi ty/cve/CVE-2024-34750 https://bugzilla.redhat.com/2295651 https://bugzilla.redha t.com/show_bug.cgi?id=2295651 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE -2024-34750 https://errata.almalinux.org/9/ALSA-2024-5693.html https://errata.ro

Vulnerability Report

ckylinux.org/RLSA-2024:5693
https://github.com/apache/tomcat
https://github.com/
apache/tomcat/commit/2344a4c0d03e307ba6b8ab6dc8b894cc8bac63f2
https://github.com
/apache/tomcat/commit/2afae300c9ac9c0e516e2e9de580847d925365c3
https://github.co
m/apache/tomcat/commit/9fec9a82887853402833a80b584e3762c7423f5f
https://linux.or
acle.com/cve/CVE-2024-34750.html
https://linux.oracle.com/errata/ELSA-2024-5694.
html
https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvplnl77y8l
https://nv
d.nist.gov/vuln/detail/CVE-2024-34750
https://security.netapp.com/advisory/ntap-
20240816-0004/
https://tomcat.apache.org/security-10.html
https://tomcat.apache.
org/security-11.html
https://tomcat.apache.org/security-9.html
https://www.cve.o
rg/CVERecord?id=CVE-2024-34750

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-50379
Title:	tomcat: RCE due to TOCTOU issue in JSP compilation
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.2, 10.1.34, 9.0.98
Source:	ghsa
Severity:	HIGH
CVSS Score:	9.8
CWE:	CWE-367
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-50379
Description:	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability during JSP compilation in Apache Tomcat permits an RCE on case insensitive file systems when the default servlet is enabled for write (non-default configuration). This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0.M1 through 9.0.97. Users are recommended to upgrade to version 11.0.2, 10.1.34 or 9.0.98, which fixes the issue.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2024/12/17/4 http://www.openwall.com/ lists/oss-security/2024/12/18/2 https://access.redhat.com/errata/RHSA-2025:3645 https://access.redhat.com/security/cve/CVE-2024-50379 https://bugzilla.redhat.co m/2332817 https://bugzilla.redhat.com/2351129 https://errata.almalinux.org/9/ALS A-2025-3645.html https://github.com/apache/tomcat https://github.com/apache/tomc at/commit/05ddeeaa54df1e2dc427d0164bedd6b79f78d81f

Vulnerability Report

https://github.com/apache/tom
cat/commit/05ddeeaa54df1e2dc427d0164bedd6b79f78d81f (10.1.34)
https://github.com
/apache/tomcat/commit/43b507ebac9d268b1ea3d908e296cc6e46795c00
https://github.co
m/apache/tomcat/commit/43b507ebac9d268b1ea3d908e296cc6e46795c00 (9.0.98)
https:/
/github.com/apache/tomcat/commit/631500b0c9b2a2a2abb707e3de2e10a5936e5d41
https:
//github.com/apache/tomcat/commit/631500b0c9b2a2a2abb707e3de2e10a5936e5d41 (9.0.
98)
https://github.com/apache/tomcat/commit/684247ae85fa633b9197b32391de59fc5470
3842
https://github.com/apache/tomcat/commit/8554f6b1722b33a2ce8b0a3fad37825f3a7
5f2d2
https://github.com/apache/tomcat/commit/8554f6b1722b33a2ce8b0a3fad37825f3a
75f2d2 (10.1.34)
https://github.com/apache/tomcat/commit/cc7a98b57c6dc1df21979fc
ff94a36e068f4456c
https://linux.oracle.com/cve/CVE-2024-50379.html
https://linux
.oracle.com/errata/ELSA-2025-3683.html
https://lists.apache.org/thread/y6lj6q1xn
p822g6ro70tn19sgtjmr80r
https://nvd.nist.gov/vuln/detail/CVE-2024-50379
https://
security.netapp.com/advisory/ntap-20250103-0003
https://security.netapp.com/advi
sory/ntap-20250103-0003/
https://tomcat.apache.org/security-10.html#Fixed_in_Apa
che_Tomcat_10.1.34
https://tomcat.apache.org/security-11.html#Fixed_in_Apache_To
mcat_11.0.2
https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0
.98
https://www.cve.org/CVERecord?id=CVE-2024-50379

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-56337
Title:	tomcat: Incomplete fix for CVE-2024-50379 - RCE due to TOCTOU issue in JSP compi lation
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.2, 10.1.34, 9.0.98
Source:	ghsa
Severity:	HIGH
CVSS Score:	N/A
CWE:	CWE-367
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-56337

Vulnerability Report

Description:	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Apache Tomcat . This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0- M1 through 10.1.33, from 9.0.0.M1 through 9.0.97. The mitigation for CVE-2024-5 0379 was incomplete. Users running Tomcat on a case insensitive file system wit h the default servlet write enabled (readonly initialisation parameter set to t he non-default value of false) may need additional configuration to fully mitiga te CVE-2024-50379 depending on which version of Java they are using with Tomcat: - running on Java 8 or Java 11: the system propertyÂ sun.io.useCanonCaches must be explicitly set to false (it defaults to true) - running on Java 17: theÂ syste m property sun.io.useCanonCaches, if set, must be set to falseÂ (it defaults to f alse) - running on Java 21 onwards: no further configuration is requiredÂ (the sy stem property and the problematic cache have been removed)

Vulnerability Report

	Tomcat 11.0.3, 10.1.
	35 and 9.0.99 onwards will include checks thatÂ sun.io.useCanonCaches is set appr
	opriately before allowing the default servlet to be write enabled on a case inse
	nsitive file system. Tomcat will also setÂ sun.io.useCanonCaches to false by defa
	ult where it can.
References:	https://access.redhat.com/security/cve/CVE-2024-56337 https://github.com/apache/ tomcat https://lists.apache.org/thread/b2b9qrgjrz1kvo4ym8y2wkfdvwoq6qbp https:// nvd.nist.gov/vuln/detail/CVE-2024-56337 https://security.netapp.com/advisory/nta p-20250103-0002 https://security.netapp.com/advisory/ntap-20250103-0002/ https:/ /tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.34 https://tomca t.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.2 https://tomcat.apach e.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.98 https://www.cve.org/CVERecor d?id=CVE-2024-50379 https://www.cve.org/CVERecord?id=CVE-2024-56337

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2020-13936
Title:	velocity: arbitrary code execution when attacker is able to modify templates
Package:	org.apache.velocity:velocity
Package ID:	org.apache.velocity:velocity:1.6.2
Installed Version:	1.6.2
Fixed Version:	N/A
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.8
CWE:	N/A
Primary URL:	https://avd.aquasec.com/nvd/cve-2020-13936
Description:	An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.

Vulnerability Report

http://www.openwall.com/lists/oss-security/2021/03/10/1

https://access.redhat.co

m/security/cve/CVE-2020-13936

https://github.com/apache/velocity-engine

https://

lists.apache.org/thread.html/r01043f584cbd47959fabe18fff64de940f81a65024bb8dddbd

a31d9a%40%3Cuser.velocity.apache.org%3E

https://lists.apache.org/thread.html/r01

043f584cbd47959fabe18fff64de940f81a65024bb8dddbda31d9a@%3Cuser.velocity.apache.o

rg%3E

https://lists.apache.org/thread.html/r0bc98e9cd080b4a13b905c571b9bed87e1a0

878d44dbf21487c6cca4%40%3Cdev.santuario.apache.org%3E

https://lists.apache.org/t

hread.html/r0bc98e9cd080b4a13b905c571b9bed87e1a0878d44dbf21487c6cca4@%3Cdev.sant

uario.apache.org%3E

https://lists.apache.org/thread.html/r17cb932fab14801b14e5b9

7a7f05192f4f366ef260c10d4a8dba8ac9%40%3Cdev.ws.apache.org%3E

https://lists.apach

e.org/thread.html/r17cb932fab14801b14e5b97a7f05192f4f366ef260c10d4a8dba8ac9@%3Cd

Vulnerability Report

ev.ws.apache.org%3E
https://lists.apache.org/thread.html/r293284c6806c73f5109800
1ea86a14271c39f72cd76af9e946d9d9ad%40%3Cdev.ws.apache.org%3E
https://lists.apach
e.org/thread.html/r293284c6806c73f51098001ea86a14271c39f72cd76af9e946d9d9ad@%3Cd
ev.ws.apache.org%3E
https://lists.apache.org/thread.html/r39de20c7e9c808b1f96790
875d33e58c9c0aabb44fd9227e7b3dc5da%40%3Cdev.ws.apache.org%3E
https://lists.apach
e.org/thread.html/r39de20c7e9c808b1f96790875d33e58c9c0aabb44fd9227e7b3dc5da@%3Cd
ev.ws.apache.org%3E
https://lists.apache.org/thread.html/r3ea4c4c908505b20a4c268
330dfe7188b90c84dcf777728d02068ae6%40%3Cannounce.apache.org%3E
https://lists.apa
che.org/thread.html/r3ea4c4c908505b20a4c268330dfe7188b90c84dcf777728d02068ae6@%3
Cannounce.apache.org%3E
https://lists.apache.org/thread.html/r4cd59453b65d4ac290
fcb3b71fdf32b4f1f8989025e89558deb5a245%40%3Cdev.ws.apache.org%3E
https://lists.a
pache.org/thread.html/r4cd59453b65d4ac290fcb3b71fdf32b4f1f8989025e89558deb5a245@
%3Cdev.ws.apache.org%3E
https://lists.apache.org/thread.html/r52a5129df402352adc
34d052bab9234c8ef63596306506a89fdc7328%40%3Cusers.activemq.apache.org%3E
https:/
/lists.apache.org/thread.html/r52a5129df402352adc34d052bab9234c8ef63596306506a89
fdc7328@%3Cusers.activemq.apache.org%3E
https://lists.apache.org/thread.html/r7f
209b837217d2a0fe5977fb692e7f15d37fa5de8214bcdc4c21d9a7%40%3Ccommits.turbine.apac
he.org%3E
https://lists.apache.org/thread.html/r7f209b837217d2a0fe5977fb692e7f15
d37fa5de8214bcdc4c21d9a7@%3Ccommits.turbine.apache.org%3E
https://lists.apache.o
rg/thread.html/r9dc2505651788ac668299774d9e7af4dc616be2f56fdc684d1170882%40%3Cus
ers.activemq.apache.org%3E
https://lists.apache.org/thread.html/r9dc2505651788ac
668299774d9e7af4dc616be2f56fdc684d1170882@%3Cusers.activemq.apache.org%3E
https:

Vulnerability Report

//lists.apache.org/thread.html/rb042f3b0090e419cc9f5a3d32cf0baff283ccd6fcb1caea6
1915d6b6%40%3Ccommits.velocity.apache.org%3E
https://lists.apache.org/thread.htm
l/rb042f3b0090e419cc9f5a3d32cf0baff283ccd6fcb1caea61915d6b6@%3Ccommits.velocity.
apache.org%3E
https://lists.apache.org/thread.html/rbee7270556f4172322936b5ecc9f
abf0c09f00d4fa56c9de1963c340%40%3Cdev.ws.apache.org%3E
https://lists.apache.org/
thread.html/rbee7270556f4172322936b5ecc9fabf0c09f00d4fa56c9de1963c340@%3Cdev.ws.
apache.org%3E
https://lists.apache.org/thread.html/rd2a89e17e8a9b451ce655f1a3411
7752ea1d18a22ce580d8baa824fd%40%3Ccommits.druid.apache.org%3E
https://lists.apac
he.org/thread.html/rd2a89e17e8a9b451ce655f1a34117752ea1d18a22ce580d8baa824fd@%3C
commits.druid.apache.org%3E
https://lists.apache.org/thread.html/rd7e865c87f9043
c21d9c1fd9d4df866061d9a08cfc322771160d8058%40%3Cdev.ws.apache.org%3E
https://lis
ts.apache.org/thread.html/rd7e865c87f9043c21d9c1fd9d4df866061d9a08cfc322771160d8
058@%3Cdev.ws.apache.org%3E
https://lists.apache.org/thread.html/re641197d204765
130618086238c73dd2ce5a3f94b33785b587d72726%40%3Cdev.ws.apache.org%3E
https://lis
ts.apache.org/thread.html/re641197d204765130618086238c73dd2ce5a3f94b33785b587d72
726@%3Cdev.ws.apache.org%3E
https://lists.apache.org/thread.html/re8e7482fe54d28
9fc0229e61cc64947b63b12c3c312e9f25bf6f3b8c%40%3Cdev.ws.apache.org%3E
https://lis
ts.apache.org/thread.html/re8e7482fe54d289fc0229e61cc64947b63b12c3c312e9f25bf6f3
b8c@%3Cdev.ws.apache.org%3E
https://lists.apache.org/thread.html/reab5978b54a9f4
c078402161e30a89c42807b198814acadbe6c862c7%40%3Cdev.ws.apache.org%3E
https://lis
ts.apache.org/thread.html/reab5978b54a9f4c078402161e30a89c42807b198814acadbe6c86
2c7@%3Cdev.ws.apache.org%3E
https://lists.apache.org/thread.html/rf7d369de88dc88
a1347006a3323b3746d849234db40a8edfd5ebc436%40%3Cdev.ws.apache.org%3E

Vulnerability Report

https://lis
ts.apache.org/thread.html/rf7d369de88dc88a1347006a3323b3746d849234db40a8edfd5ebc
436@%3Cdev.ws.apache.org%3E
https://lists.debian.org/debian-lts-announce/2021/03
/msg00019.html
https://nvd.nist.gov/vuln/detail/CVE-2020-13936
https://security.
gentoo.org/glsa/202107-52
https://ubuntu.com/security/notices/USN-6281-1
https:/
/www.cve.org/CVERecord?id=CVE-2020-13936
https://www.openwall.com/lists/oss-secu
rity/2021/03/10/1
https://www.oracle.com/security-alerts/cpuapr2022.html
https:/
/www.oracle.com/security-alerts/cpujan2022.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-45688
Title:	json stack overflow vulnerability
Package:	org.json:json
Package ID:	org.json:json:20171018
Installed Version:	20171018
Fixed Version:	20230227
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-787
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-45688
Description:	A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.
References:	https://github.com/dromara/hutool/commit/6a2b585de0a380e8c12016dbaa1620b69be11b8c https://github.com/dromara/hutool/issues/2748 https://github.com/dromara/hutool/releases/tag/5.8.25 https://github.com/stleary/JSON-java/commit/a6e412bded7a0ad605adfeca029318f184c32102 https://github.com/stleary/JSON-java/issues/708 https://nvd.nist.gov/vuln/detail/CVE-2022-45688

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-5072
Title:	JSON-java: parser confusion leads to OOM
Package:	org.json:json
Package ID:	org.json:json:20171018
Installed Version:	20171018
Fixed Version:	20231013
Source:	ghsa
Severity:	HIGH
CVSS Score:	N/A
CWE:	CWE-770
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-5072
Description:	Denial of Service in JSON-Java versions up to and including 20230618. Â A bug in the parser means that an input string of modest size can lead to indefinite amounts of memory being used.
References:	http://www.openwall.com/lists/oss-security/2023/12/13/4 https://access.redhat.com/security/cve/CVE-2023-5072 https://github.com/google/security-research/security/advisories/GHSA-4jq9-2xhw-jpx7 https://github.com/stleary/JSON-java https://github.com/stleary/JSON-java/commit/60662e2f8384d3449822a3a1179bfe8de67b55bb https://github.com/stleary/JSON-java/issues/758 https://github.com/stleary/JSON-java/issues/771 https://github.com/stleary/JSON-java/pull/759 https://nvd.nist.gov/vuln/detail/CVE-2023-5072 https://security.netapp.com/advisory/ntap-20240621-0007/ https://www.cve.org/CVERecord?id=CVE-2023-5072

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-37714
Title:	jsoup: Crafted input may cause the jsoup HTML and XML parser to get stuck
Package:	org.jsoup:jsoup
Package ID:	org.jsoup:jsoup:1.10.2
Installed Version:	1.10.2
Fixed Version:	1.14.2
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-248, CWE-835
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-37714
Description:	jsoup is a Java library for working with HTML. Those using jsoup versions prior to 1.14.2 to parse untrusted HTML or XML may be vulnerable to DOS attacks. If th e parser is run on user supplied input, an attacker may supply content that caus es the parser to get stuck (loop indefinitely until cancelled), to complete more slowly than usual, or to throw an unexpected exception. This effect may support a denial of service attack. The issue is patched in version 1.14.2. There are a few available workarounds. Users may rate limit input parsing, limit the size o f inputs based on system resources, and/or implement thread watchdogs to cap and timeout parse runtimes.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2021-37714 https://github.com/jhy/jso up https://github.com/jhy/jsoup/security/advisories/GHSA-m72m-mhq2-9p6c https:// jsoup.org/news/release-1.14.1 https://jsoup.org/news/release-1.14.2 https://list s.apache.org/thread.html/r215009dbf7467a9f6506d0c0024cb36cad30071010e62c9352cfaa f0%40%3Cissues.maven.apache.org%3E https://lists.apache.org/thread.html/r215009d bf7467a9f6506d0c0024cb36cad30071010e62c9352cfaaf0@%3Cissues.maven.apache.org%3E https://lists.apache.org/thread.html/r377b93d79817ce649e9e68b3456e6f499747ef1643 fa987b342e082e%40%3Cissues.maven.apache.org%3E

Vulnerability Report

https://lists.apache.org/thread.h
tml/r377b93d79817ce649e9e68b3456e6f499747ef1643fa987b342e082e@%3Cissues.maven.ap
ache.org%3E
https://lists.apache.org/thread.html/r3d71f18adb78e50f626dde689161ca
63d3b7491bd9718fcddfaecba7%40%3Cissues.maven.apache.org%3E
https://lists.apache.
org/thread.html/r3d71f18adb78e50f626dde689161ca63d3b7491bd9718fcddfaecba7@%3Ciss
ues.maven.apache.org%3E
https://lists.apache.org/thread.html/r50e9c9466c592ca9d7
07a5dea549524d19e3287da08d8392f643960e%40%3Cissues.maven.apache.org%3E
https://l
ists.apache.org/thread.html/r50e9c9466c592ca9d707a5dea549524d19e3287da08d8392f64
3960e@%3Cissues.maven.apache.org%3E
https://lists.apache.org/thread.html/r685c52
35235ad0c26e86d0ee987fb802c9675de6081dbf0516464e0b%40%3Cnotifications.james.apac
he.org%3E
https://lists.apache.org/thread.html/r685c5235235ad0c26e86d0ee987fb802
c9675de6081dbf0516464e0b@%3Cnotifications.james.apache.org%3E
https://lists.apac
he.org/thread.html/r97404676a5cf591988faedb887d64e278f522adcaa823d89ca69defe%40%
3Cnotifications.james.apache.org%3E
https://lists.apache.org/thread.html/r974046
76a5cf591988faedb887d64e278f522adcaa823d89ca69defe@%3Cnotifications.james.apache
.org%3E
https://lists.apache.org/thread.html/rc3354080fc67fb50b45b3c2d12dc4ca2a3
c1c78dad3d3ba012c038aa%40%3Cnotifications.james.apache.org%3E
https://lists.apac
he.org/thread.html/rc3354080fc67fb50b45b3c2d12dc4ca2a3c1c78dad3d3ba012c038aa@%3C
notifications.james.apache.org%3E
https://nvd.nist.gov/vuln/detail/CVE-2021-3771
4
https://security.netapp.com/advisory/ntap-20220210-0022
https://security.netap
p.com/advisory/ntap-20220210-0022/
https://www.cve.org/CVERecord?id=CVE-2021-377
14
https://www.oracle.com/security-alerts/cpuapr2022.html

Vulnerability Report

https://www.oracle.com
/security-alerts/cpujan2022.html
https://www.oracle.com/security-alerts/cpujul20
22.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2025-22235
Title:	org.springframework.boot/spring-boot: Spring Boot EndpointRequest.to() creates w rong matcher if actuator endpoint is not exposed
Package:	org.springframework.boot:spring-boot
Package ID:	org.springframework.boot:spring-boot:2.6.2
Installed Version:	2.6.2
Fixed Version:	3.3.11, 3.4.5
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.3
CWE:	CWE-20
Primary URL:	https://avd.aquasec.com/nvd/cve-2025-22235

Vulnerability Report

Description:	EndpointRequest.to()Â creates a matcher for null/**Â if the actuator endpoint, for which the EndpointRequestÂ has been created, is disabled or not exposed. Your a pplication may be affected by this if all the following conditions are met: * You use Spring Security * EndpointRequest.to()Â has been used in a Spring Se curity chain configuration * The endpoint which EndpointRequestÂ references is disabled or not exposed via web * Your application handles requests to /null Â and this path needs protection You are not affected if any of the following i s true: * You don't use Spring Security * You don't use EndpointRequest.t o() * The endpoint which EndpointRequest.to()Â refers to is enabled and is exp

Vulnerability Report

	osed
	* Your application does not handle requests to /nullÂ or this path does n
	ot need protection
References:	https://access.redhat.com/security/cve/CVE-2025-22235 https://github.com/advisor ies/GHSA-rc42-6c7j-7h5r https://github.com/spring-projects/spring-boot https://n vd.nist.gov/vuln/detail/CVE-2025-22235 https://security.netapp.com/advisory/ntap -20250516-0010 https://security.netapp.com/advisory/ntap-20250516-0010/ https:// spring.io/security/cve-2025-22235 https://www.cve.org/CVERecord?id=CVE-2025-2223 5

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-20883
Title:	spring-boot: Spring Boot Welcome Page DoS Vulnerability
Package:	org.springframework.boot:spring-boot-autoconfigure
Package ID:	org.springframework.boot:spring-boot-autoconfigure:2.6.2
Installed Version:	2.6.2
Fixed Version:	3.0.7, 2.7.12, 2.6.15, 2.5.15
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-400
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-20883
Description:	In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2 .5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.
References:	https://access.redhat.com/security/cve/CVE-2023-20883 https://github.com/spring-projects/spring-boot https://github.com/spring-projects/spring-boot/commit/418dd1ba5bdad79b55a043000164bfcbda2acd78 https://github.com/spring-projects/spring-boot/issues/35552 https://github.com/spring-projects/spring-boot/releases/tag/v2.5.15 https://github.com/spring-projects/spring-boot/releases/tag/v2.6.15 https://github.com/spring-projects/spring-boot/releases/tag/v2.7.12 https://nvd.nist.gov/vuln/detail/CVE-2023-20883 https://security.netapp.com/advisory/ntap-20230703-0008 https://security.netapp.com/advisory/ntap-20230703-0008/ https://spring.io/security/cve-2023-20883 https://www.cve.org/CVERecord?id=CVE-2023-20883

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-22970
Title:	springframework: DoS via data binding to multipartFile or servlet part
Package:	org.springframework:spring-beans
Package ID:	org.springframework:spring-beans:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.2.22.RELEASE, 5.3.20
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-770
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-22970
Description:	In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported vers ions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.
References:	https://access.redhat.com/security/cve/CVE-2022-22970 https://github.com/spring- projects/spring-framework https://github.com/spring-projects/spring-framework/co mmit/50177b1ad3485bd44239b1756f6c14607476fcf2 https://github.com/spring-projects /spring-framework/commit/83186b689f11f5e6efe7ccc08fdeb92f66fcd583 https://nvd.ni st.gov/vuln/detail/CVE-2022-22970 https://security.netapp.com/advisory/ntap-2022 0616-0006 https://security.netapp.com/advisory/ntap-20220616-0006/ https://tanzu .vmware.com/security/cve-2022-22970 https://www.cve.org/CVERecord?id=CVE-2022-22 970 https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-22968
Title:	Framework: Data Binding Rules Vulnerability
Package:	org.springframework:spring-context
Package ID:	org.springframework:spring-context:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.3.19, 5.2.21.RELEASE
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-178
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-22968
Description:	In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path .
References:	https://access.redhat.com/security/cve/CVE-2022-22968 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/commit/833e750175349ab4fd502109a8b41af77e25cdea https://github.com/spring-projects/spring-framework/commit/a7cf19cec5ebd270f97a194d749e2d5701ad2ab7 https://nvd.nist.gov/vuln/detail/CVE-2022-22968 https://security.netapp.com/advisory/ntap-20220602-0004 https://security.netapp.com/advisory/ntap-20220602-0004/ https://tanzu.vmware.com/security/cve-2022-22968 https://www.cve.org/CVERecord?id=CVE-2022-22968 https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-20863
Title:	springframework: Spring Expression DoS Vulnerability
Package:	org.springframework:spring-expression
Package ID:	org.springframework:spring-expression:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.0.8, 5.3.27, 5.2.24.RELEASE
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-400, CWE-917
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-20863
Description:	In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it i s possible for a user to provide a specially crafted SpEL expression that may ca use a denial-of-service (DoS) condition.
References:	https://access.redhat.com/security/cve/CVE-2023-20863 https://github.com/spring- projects/spring-framework https://github.com/spring-projects/spring-framework/co mmit/965a6392757d20f9db19241126fcc719a51eac15 https://github.com/spring-projects /spring-framework/commit/b73f5fcac22555f844cf27a7eeb876cb9d7f7f7e https://github .com/spring-projects/spring-framework/commit/ebc82654282bda547fbc20a9749ab1bda88 6a46f https://nvd.nist.gov/vuln/detail/CVE-2023-20863 https://security.netapp.co m/advisory/ntap-20240524-0015 https://security.netapp.com/advisory/ntap-20240524 -0015/ https://spring.io/security/cve-2023-20863 https://www.cve.org/CVERecord?i d=CVE-2023-20863

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-22243
Title:	springframework: URL Parsing with Host Validation
Package:	org.springframework:spring-web
Package ID:	org.springframework:spring-web:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.1.4, 6.0.17, 5.3.32
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.1
CWE:	CWE-601
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-22243
Description:	Applications that use UriComponentsBuilderÂ to parse an externally provided URL (e.g. through a query parameter) ANDÂ perform validation checks on the host of the parsed URL may be vulnerable to a open redirect https://cwe.mitre.org/data/definitions/601.html Â attack or to a SSRF attack if the URL is used after passing validation checks.
References:	http://seclists.org/fulldisclosure/2024/Sep/24 https://access.redhat.com/security/cve/CVE-2024-22243 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/blob/main/spring-web/src/main/java/org/springframework/web/util/UriComponentsBuilder.java https://nvd.nist.gov/vuln/detail/CVE-2024-22243 https://security.netapp.com/advisory/ntap-20240524-0001 https://security.netapp.com/advisory/ntap-20240524-0001/ https://spring.io/security/cve-2024-22243 https://www.cve.org/CVERecord?id=CVE-2024-22243

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-22259
Title:	springframework: URL Parsing with Host Validation
Package:	org.springframework:spring-web
Package ID:	org.springframework:spring-web:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.1.5, 6.0.18, 5.3.33
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.1
CWE:	CWE-601
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-22259
Description:	Applications that use UriComponentsBuilder in Spring FrameworkÂ to parse an exter nally provided URL (e.g. through a query parameter) ANDÂ perform validation check s on the host of the parsed URL may be vulnerable to a open redirect https://cw e.mitre.org/data/definitions/601.html Â attack or to a SSRF attack if the URL is used after passing validation checks. This is the same as CVE-2024-22243 https ://spring.io/security/cve-2024-22243 , but with different input.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2024-22259 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/commit/297cbae2990e1413537c55845a7e0ea0ffd9f9bb https://github.com/spring-projects/spring-framework/commit/381f790329a48b74c2a49fc1384dd68ca9153501 https://github.com/spring-projects/spring-framework/commit/f2fd2f12269c6a781c5b2c20b3c24141055a3d68 https://nvd.nist.gov/vuln/detail/CVE-2024-22259 https://security.netapp.com/advisory/ntap-20240524-0002 https://security.netapp.com/advisory/ntap-20240524-0002/ https://spring.io/security/cve-2024-22259

Vulnerability Report

https://www.cve.org/CVERecord?i
d=CVE-2024-22259

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-22262
Title:	springframework: URL Parsing with Host Validation
Package:	org.springframework:spring-web
Package ID:	org.springframework:spring-web:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.3.34, 6.0.19, 6.1.6
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.1
CWE:	CWE-601, CWE-918
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-22262
Description:	Applications that use UriComponentsBuilderÂ to parse an externally provided URL (e.g. through a query parameter) ANDÂ perform validation checks on the host of the parsed URL may be vulnerable to a open redirect https://cwe.mitre.org/data/definitions/601.html Â attack or to a SSRF attack if the URL is used after passing validation checks. This is the same as CVE-2024-22259 https://spring.io/security/cve-2024-22259 Â and CVE-2024-22243 https://spring.io/security/cve-2024-22243 , but with different input.
References:	https://access.redhat.com/security/cve/CVE-2024-22262 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/blob/main/spring-web/src/main/java/org/springframework/web/util/UriComponentsBuilder.java https://nvd.nist.gov/vuln/detail/CVE-2024-22262 https://security.netapp.com/advisory/ntap-20240524-0003 https://security.netapp.com/advisory/ntap-20240524-0003/ https://spring.io/security/cve-2024-22262 https://www.cve.org/CVERecord?id=CVE-2024-22262

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-38816
Title:	spring-webmvc: Path Traversal Vulnerability in Spring Applications Using RouterFunctions and FileSystemResource
Package:	org.springframework:spring-webmvc
Package ID:	org.springframework:spring-webmvc:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.1.13
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-22
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-38816
Description:	Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks. An attacker can craft malicious HTTP requests and obtain any file on the file system that is also accessible to the process in which the Spring application is running. Specifically, an application is vulnerable when both of the following are true: * the web application uses RouterFunctionsÂ to serve static resources * resource handling is explicitly configured with a FileSystemResourceÂ location However, malicious requests are blocked and rejected when any of the following is true: * the Spring Security HTTP Firewall https://docs.spring.io/spring-security/reference/servlet/exploits/firewall.html Â is in use * the application runs on Tomcat or Jetty

Vulnerability Report

References:

https://access.redhat.com/security/cve/CVE-2024-38816

Vulnerability Report

https://github.com/spring-
projects/spring-framework
https://github.com/spring-projects/spring-framework/co
mmit/d86bf8b2056429edf5494456cffcb2b243331c49
https://nvd.nist.gov/vuln/detail/C
VE-2024-38816
https://security.netapp.com/advisory/ntap-20241227-0001
https://se
curity.netapp.com/advisory/ntap-20241227-0001/
https://spring.io/security/cve-20
24-38816
https://www.cve.org/CVERecord?id=CVE-2024-38816

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-38819
Title:	org.springframework:spring-webmvc: Path traversal vulnerability in functional we b frameworks
Package:	org.springframework:spring-webmvc
Package ID:	org.springframework:spring-webmvc:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.1.14
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-22
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-38819
Description:	Applications serving static resources through the functional web frameworks WebM vc.fn or WebFlux.fn are vulnerable to path traversal attacks. An attacker can cr aft malicious HTTP requests and obtain any file on the file system that is also accessible to the process in which the Spring application is running.
References:	https://access.redhat.com/security/cve/CVE-2024-38819 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/commit/3bfbe30a7814c9ea1556d40df9bd87ddb3ba372d https://github.com/spring-projects/spring-framework/commit/fb7890d73975a3d9e0763e0926df2bd0a608e87e https://github.com/spring-projects/spring-framework/issues/33689 https://nvd.nist.gov/vuln/detail/CVE-2024-38819 https://security.netapp.com/advisory/ntap-20250110-0010 https://security.netapp.com/advisory/ntap-20250110-0010/ https://spring.io/security/cve-2024-38819 https://www.cve.org/CVERecord?id=CVE-2024-38819

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-1471
Title:	SnakeYaml: Constructor Deserialization Remote Code Execution
Package:	org.yaml:snakeyaml
Package ID:	org.yaml:snakeyaml:1.29
Installed Version:	1.29
Fixed Version:	2.0
Source:	ghsa
Severity:	HIGH
CVSS Score:	8.3
CWE:	CWE-20, CWE-502
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-1471
Description:	SnakeYaml's Constructor() class does not restrict types which can be instantiate d during deserialization.Â Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor w hen parsing untrusted content to restrict deserialization. We recommend upgradin g to version 2.0 and beyond.

Vulnerability Report

References:	http://packetstormsecurity.com/files/175095/PyTorch-Model-Server-Registration-De serialization-Remote-Code-Execution.html http://www.openwall.com/lists/oss-secur ity/2023/11/19/1 https://access.redhat.com/errata/RHSA-2022:9058 https://access. redhat.com/security/cve/CVE-2022-1471 https://bitbucket.org/snakeyaml/snakeyaml https://bitbucket.org/snakeyaml/snakeyaml/commits/5014df1a36f50aca54405bb8433bc9 9a8847f758 https://bitbucket.org/snakeyaml/snakeyaml/commits/acc44099f5f4af26ff8 6b4e4e4cc1c874e2dc5c4 https://bitbucket.org/snakeyaml/snakeyaml/issues/561/cve-2 022-1471-vulnerability-in#comment-64581479 https://bitbucket.org/snakeyaml/snake yaml/issues/561/cve-2022-1471-vulnerability-in#comment-64634374 https://bitbucke t.org/snakeyaml/snakeyaml/issues/561/cve-2022-1471-vulnerability-in#comment-6487

Vulnerability Report

6314
https://bitbucket.org/snakeyaml/snakeyaml/wiki/CVE-2022-1471
https://bugzil
la.redhat.com/2150009
https://bugzilla.redhat.com/show_bug.cgi?id=2150009
https:
//cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1471
https://errata.almalinux.
org/8/ALSA-2022-9058.html
https://errata.rockylinux.org/RLSA-2022:9058
https://g
ithub.com/google/security-research/security/advisories/GHSA-mjmj-j48q-9wg2
https
://github.com/mbechler/marshalsec
https://groups.google.com/g/kubernetes-securit
y-announce/c/mwrakFaEdnc
https://linux.oracle.com/cve/CVE-2022-1471.html
https:/
/linux.oracle.com/errata/ELSA-2022-9058-1.html
https://nvd.nist.gov/vuln/detail/
CVE-2022-1471
https://security.netapp.com/advisory/ntap-20230818-0015
https://se
curity.netapp.com/advisory/ntap-20230818-0015/
https://security.netapp.com/advis
ory/ntap-20240621-0006
https://security.netapp.com/advisory/ntap-20240621-0006/
https://snyk.io/blog/unsafe-deserialization-snakeyaml-java-cve-2022-1471
https:/
/www.cve.org/CVERecord?id=CVE-2022-1471
https://www.github.com/mbechler/marshals
ec/blob/master/marshalsec.pdf?raw=true

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-25857
Title:	snakeyaml: Denial of Service due to missing nested depth limitation for collecti ons
Package:	org.yaml:snakeyaml
Package ID:	org.yaml:snakeyaml:1.29
Installed Version:	1.29
Fixed Version:	1.31
Source:	ghsa
Severity:	HIGH
CVSS Score:	7.5
CWE:	CWE-776
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-25857
Description:	The package org.yaml:snakeyaml from 0 and before 1.31 are vulnerable to Denial o f Service (DoS) due missing to nested depth limitation for collections.

Vulnerability Report

References:	https://access.redhat.com/errata/RHSA-2022:6820 https://access.redhat.com/securi ty/cve/CVE-2022-25857 https://bitbucket.org/snakeyaml/snakeyaml/commits/fc300780 da21f4bb92c148bc90257201220cf174 https://bitbucket.org/snakeyaml/snakeyaml/issue s/525 https://bugzilla.redhat.com/2126789 https://bugzilla.redhat.com/show_bug.c gi?id=2126789 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25857 http s://errata.almalinux.org/8/ALSA-2022-6820.html https://errata.rockylinux.org/RLS A-2022:6820 https://github.com/snakeyaml/snakeyaml https://github.com/snakeyaml/ snakeyaml/commit/fc300780da21f4bb92c148bc90257201220cf174 https://linux.oracle.c om/cve/CVE-2022-25857.html https://linux.oracle.com/errata/ELSA-2022-6820.html

Vulnerability Report

h
ttps://lists.debian.org/debian-lts-announce/2022/10/msg00001.html
https://nvd.ni
st.gov/vuln/detail/CVE-2022-25857
https://security.netapp.com/advisory/ntap-2024
0315-0010
https://security.netapp.com/advisory/ntap-20240315-0010/
https://secur
ity.snyk.io/vuln/SNYK-JAVA-ORGYAML-2806360
https://ubuntu.com/security/notices/U
SN-5944-1
https://www.cve.org/CVERecord?id=CVE-2022-25857

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-12798
Title:	logback-core: arbitrary code execution via JaninoEventEvaluator
Package:	ch.qos.logback:logback-core
Package ID:	ch.qos.logback:logback-core:1.2.9
Installed Version:	1.2.9
Fixed Version:	1.5.13, 1.3.15
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	N/A
CWE:	CWE-917
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-12798

Vulnerability Report

Description:	ACE vulnerability in JaninoEventEvaluator by QOS.CH logback-core upto inc luding version 0.1 to 1.3.14 andÂ 1.4.0 to 1.5.12 in Java applications allows attacker to execute arbitrary code by compromising an existing logback configuration file or by injecting an environment variable before program execution. Malicious logback configuration files can allow the attacker to execute arbitrary code using the JaninoEventEvaluator extension. A successfu l attack requires the user to have write access to a configuration file. Altern atively, the attacker could inject a malicious

Vulnerability Report

	environment variable pointing to
	a malicious configuration file. In both
	cases, the attack requires existing pr
	ivilege.
References:	https://access.redhat.com/security/cve/CVE-2024-12798 https://github.com/qos-ch/ logback https://github.com/qos-ch/logback/commit/2cb6d520df7592ef1c3a198f1b5df3c 10c93e183 https://logback.qos.ch/news.html#1.3.15 https://logback.qos.ch/news.ht ml#1.5.13 https://nvd.nist.gov/vuln/detail/CVE-2024-12798 https://www.cve.org/CV ERecord?id=CVE-2024-12798

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-29425
Title:	apache-commons-io: Limited path traversal in Apache Commons IO 2.2 to 2.6
Package:	commons-io:commons-io
Package ID:	commons-io:commons-io:2.3
Installed Version:	2.3
Fixed Version:	2.7
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	4.8
CWE:	CWE-20, CWE-22
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-29425
Description:	In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normaliz e with an improper input string, like "//../foo", or "\\..\foo", the result woul d be the same value, thus possibly providing access to files in the parent direc tory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.

Vulnerability Report

https://access.redhat.com/security/cve/CVE-2021-29425

https://arxiv.org/pdf/2306

.05534.pdf

https://github.com/jensdietrich/xshady-release/tree/main/CVE-2021-294

25

https://issues.apache.org/jira/browse/IO-556

https://lists.apache.org/thread.

html/r01b4a1fcdf3311c936ce33d75a9398b6c255f00c1a2f312ac21effe1%40%3Cnotification

s.zookeeper.apache.org%3E

https://lists.apache.org/thread.html/r01b4a1fcdf3311c9

36ce33d75a9398b6c255f00c1a2f312ac21effe1@%3Cnotifications.zookeeper.apache.org%3

E

https://lists.apache.org/thread.html/r0bfa8f7921abdfae788b1f076a12f73a92c93cc0

a6e1083bce0027c5%40%3Cnotifications.zookeeper.apache.org%3E

https://lists.apache

.org/thread.html/r0bfa8f7921abdfae788b1f076a12f73a92c93cc0a6e1083bce0027c5@%3Cno

tifications.zookeeper.apache.org%3E

https://lists.apache.org/thread.html/r0d73e2

071d1f1afe1a15da14c5b6feb2cf17e3871168d5a3c8451436%40%3Ccommits.pulsar.apache.or

g%3E
https://lists.apache.org/thread.html/r0d73e2071d1f1afe1a15da14c5b6feb2cf17e
3871168d5a3c8451436@%3Ccommits.pulsar.apache.org%3E
https://lists.apache.org/thr
ead.html/r1c2f4683c35696cf6f863e3c107e37ec41305b1930dd40c17260de71%40%3Ccommits.
pulsar.apache.org%3E
https://lists.apache.org/thread.html/r1c2f4683c35696cf6f863
e3c107e37ec41305b1930dd40c17260de71@%3Ccommits.pulsar.apache.org%3E
https://list
s.apache.org/thread.html/r20416f39ca7f7344e7d76fe4d7063bb1d91ad106926626e7e83fb3
46%40%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.org/thread.ht
ml/r20416f39ca7f7344e7d76fe4d7063bb1d91ad106926626e7e83fb346@%3Cnotifications.zo
okeeper.apache.org%3E
https://lists.apache.org/thread.html/r2345b49dbffa8a5c3c58
9c082fe39228a2c1d14f11b96c523da701db%40%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.org/thread.html/r2345b49dbffa8a5c3c589c082fe39228a2c1d14f11
b96c523da701db@%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.org
/thread.html/r2721aba31a8562639c4b937150897e24f78f747cdbda8641c0f659fe%40%3Cuser
s.kafka.apache.org%3E
https://lists.apache.org/thread.html/r2721aba31a8562639c4b
937150897e24f78f747cdbda8641c0f659fe@%3Cusers.kafka.apache.org%3E
https://lists.
apache.org/thread.html/r27b1eedda37468256c4bb768fde1e8b79b37ec975cbbfd0d65a7ac34
%40%3Cdev.myfaces.apache.org%3E
https://lists.apache.org/thread.html/r27b1eedda3
7468256c4bb768fde1e8b79b37ec975cbbfd0d65a7ac34@%3Cdev.myfaces.apache.org%3E
http
s://lists.apache.org/thread.html/r2bc986a070457daca457a54fe71ee09d2584c24dc26233
6ca32b6a19%40%3Cdev.creadur.apache.org%3E
https://lists.apache.org/thread.html/r
2bc986a070457daca457a54fe71ee09d2584c24dc262336ca32b6a19@%3Cdev.creadur.apache.o
rg%3E
https://lists.apache.org/thread.html/r2df50af2641d38f432ef025cd2ba5858215c
c0cf3fc10396a674ad2e%40%3Cpluto-scm.portals.apache.org%3E

Vulnerability Report

https://lists.apache.o
rg/thread.html/r2df50af2641d38f432ef025cd2ba5858215cc0cf3fc10396a674ad2e@%3Cplut
o-scm.portals.apache.org%3E
https://lists.apache.org/thread.html/r345330b7858304
938b7b8029d02537a116d75265a598c98fa333504a%40%3Cdev.creadur.apache.org%3E
https:
//lists.apache.org/thread.html/r345330b7858304938b7b8029d02537a116d75265a598c98f
a333504a@%3Cdev.creadur.apache.org%3E
https://lists.apache.org/thread.html/r4050
f9f6b42ebfa47a98cbdee4aabed4bb5fb8093db7dbb88faceba2%40%3Ccommits.zookeeper.apac
he.org%3E
https://lists.apache.org/thread.html/r4050f9f6b42ebfa47a98cbdee4aabed4
bb5fb8093db7dbb88faceba2@%3Ccommits.zookeeper.apache.org%3E
https://lists.apache
.org/thread.html/r462db908acc1e37c455e11b1a25992b81efd18e641e7e0ceb1b6e046%40%3C
notifications.zookeeper.apache.org%3E
https://lists.apache.org/thread.html/r462d
b908acc1e37c455e11b1a25992b81efd18e641e7e0ceb1b6e046@%3Cnotifications.zookeeper.
apache.org%3E
https://lists.apache.org/thread.html/r477c285126ada5c3b47946bb702c
b222ac4e7fd3100c8549bdd6d3b2%40%3Cissues.zookeeper.apache.org%3E
https://lists.a
pache.org/thread.html/r477c285126ada5c3b47946bb702cb222ac4e7fd3100c8549bdd6d3b2@
%3Cissues.zookeeper.apache.org%3E
https://lists.apache.org/thread.html/r47ab6f68
cbba8e730f42c4ea752f3a44eb95fb09064070f2476bb401%40%3Cdev.creadur.apache.org%3E
https://lists.apache.org/thread.html/r47ab6f68cbba8e730f42c4ea752f3a44eb95fb0906
4070f2476bb401@%3Cdev.creadur.apache.org%3E
https://lists.apache.org/thread.html
/r5149f78be265be69d34eacb4e4b0fc7c9c697bcdfa91a1c1658d717b%40%3Cissues.zookeeper
.apache.org%3E
https://lists.apache.org/thread.html/r5149f78be265be69d34eacb4e4b
0fc7c9c697bcdfa91a1c1658d717b@%3Cissues.zookeeper.apache.org%3E
https://lists.ap
ache.org/thread.html/r523a6ffad58f71c4f3761e3cee72df878e48cdc89ebdce933be1475c%4
0%3Cdev.creadur.apache.org%3E

Vulnerability Report

https://lists.apache.org/thread.html/r523a6ffad58f
71c4f3761e3cee72df878e48cdc89ebdce933be1475c@%3Cdev.creadur.apache.org%3E
https:
//lists.apache.org/thread.html/r808be7d93b17a7055c1981a8453ae5f0d0fce5855407793c
5d0ffffa%40%3Cuser.commons.apache.org%3E
https://lists.apache.org/thread.html/r8
08be7d93b17a7055c1981a8453ae5f0d0fce5855407793c5d0ffffa@%3Cuser.commons.apache.o
rg%3E
https://lists.apache.org/thread.html/r8569a41d565ca880a4dee0e645dad1cd17ab
4a92e68055ad9ebb7375%40%3Cdev.creadur.apache.org%3E
https://lists.apache.org/thr
ead.html/r8569a41d565ca880a4dee0e645dad1cd17ab4a92e68055ad9ebb7375@%3Cdev.creadu
r.apache.org%3E
https://lists.apache.org/thread.html/r86528f4b7d222aed7891e7ac03
d69a0db2a2dfa17b86ac3470d7f374%40%3Cnotifications.zookeeper.apache.org%3E
https:
//lists.apache.org/thread.html/r86528f4b7d222aed7891e7ac03d69a0db2a2dfa17b86ac34
70d7f374@%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.org/threa
d.html/r873d5ddafc0a68fd999725e559776dc4971d1ab39c0f5cc81bd9bc04%40%3Ccommits.pu
lsar.apache.org%3E
https://lists.apache.org/thread.html/r873d5ddafc0a68fd999725e
559776dc4971d1ab39c0f5cc81bd9bc04@%3Ccommits.pulsar.apache.org%3E
https://lists.
apache.org/thread.html/r8bfc7235e6b39d90e6f446325a5a44c3e9e50da18860fdabcee23e29
%40%3Cissues.zookeeper.apache.org%3E
https://lists.apache.org/thread.html/r8bfc7
235e6b39d90e6f446325a5a44c3e9e50da18860fdabcee23e29@%3Cissues.zookeeper.apache.o
rg%3E
https://lists.apache.org/thread.html/r8efcbabde973ea72f5e0933adc48ef1425db
5cde850bf641b3993f31%40%3Cdev.commons.apache.org%3E
https://lists.apache.org/thr
ead.html/r8efcbabde973ea72f5e0933adc48ef1425db5cde850bf641b3993f31@%3Cdev.common
s.apache.org%3E
https://lists.apache.org/thread.html/r92ea904f4bae190b03bd42a435
5ce3c2fbe8f36ab673e03f6ca3f9fa%40%3Cnotifications.zookeeper.apache.org%3E
https:

Vulnerability Report

//lists.apache.org/thread.html/r92ea904f4bae190b03bd42a4355ce3c2fbe8f36ab673e03f
6ca3f9fa@%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.org/threa
d.html/ra8ef65aedc086d2d3d21492b4c08ae0eb8a3a42cc52e29ba1bc009d8%40%3Cdev.creadu
r.apache.org%3E
https://lists.apache.org/thread.html/ra8ef65aedc086d2d3d21492b4c
08ae0eb8a3a42cc52e29ba1bc009d8@%3Cdev.creadur.apache.org%3E
https://lists.apache
.org/thread.html/raa053846cae9d497606027816ae87b4e002b2e0eb66cb0dee710e1f5%40%3C
dev.creadur.apache.org%3E
https://lists.apache.org/thread.html/raa053846cae9d497
606027816ae87b4e002b2e0eb66cb0dee710e1f5@%3Cdev.creadur.apache.org%3E
https://li
sts.apache.org/thread.html/rad4ae544747df32ccd58fff5a86cd556640396aeb161aa71dd3d
192a%40%3Cuser.commons.apache.org%3E
https://lists.apache.org/thread.html/rad4ae
544747df32ccd58fff5a86cd556640396aeb161aa71dd3d192a@%3Cuser.commons.apache.org%3
E
https://lists.apache.org/thread.html/rbebd3e19651baa7a4a5503a9901c95989df9d406
02c8e35cb05d3eb5%40%3Cdev.creadur.apache.org%3E
https://lists.apache.org/thread.
html/rbebd3e19651baa7a4a5503a9901c95989df9d40602c8e35cb05d3eb5@%3Cdev.creadur.ap
ache.org%3E
https://lists.apache.org/thread.html/rc10fa20ef4d13cbf6ebe0b06b5edb9
5466a1424a9b7673074ed03260%40%3Cnotifications.zookeeper.apache.org%3E
https://li
sts.apache.org/thread.html/rc10fa20ef4d13cbf6ebe0b06b5edb95466a1424a9b7673074ed0
3260@%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.org/thread.ht
ml/rc2dd3204260e9227a67253ef68b6f1599446005bfa0e1ddce4573a80%40%3Cpluto-dev.port
als.apache.org%3E
https://lists.apache.org/thread.html/rc2dd3204260e9227a67253ef
68b6f1599446005bfa0e1ddce4573a80@%3Cpluto-dev.portals.apache.org%3E
https://list
s.apache.org/thread.html/rc359823b5500e9a9a2572678ddb8e01d3505a7ffcadfa8d13b8780
ab%40%3Cuser.commons.apache.org%3E
https://lists.apache.org/thread.html/rc5f3df5

Vulnerability Report

316c5237b78a3dff5ab95b311ad08e61d418cd992ca7e34ae%40%3Cnotifications.zookeeper.a
pache.org%3E
https://lists.apache.org/thread.html/rc5f3df5316c5237b78a3dff5ab95b
311ad08e61d418cd992ca7e34ae@%3Cnotifications.zookeeper.apache.org%3E
https://lis
ts.apache.org/thread.html/rc65f9bc679feffe4589ea0981ee98bc0af9139470f077a91580ee
ee0%40%3Cpluto-dev.portals.apache.org%3E
https://lists.apache.org/thread.html/rc
65f9bc679feffe4589ea0981ee98bc0af9139470f077a91580eeee0@%3Cpluto-dev.portals.apa
che.org%3E
https://lists.apache.org/thread.html/rca71a10ca533eb9bfac2d590533f02e
6fb9064d3b6aa3ec90fdc4f51%40%3Cnotifications.zookeeper.apache.org%3E
https://lis
ts.apache.org/thread.html/rca71a10ca533eb9bfac2d590533f02e6fb9064d3b6aa3ec90fdc4
f51@%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.org/thread.htm
l/rd09d4ab3e32e4b3a480e2ff6ff118712981ca82e817f28f2a85652a6%40%3Cnotifications.z
ookeeper.apache.org%3E
https://lists.apache.org/thread.html/rd09d4ab3e32e4b3a480
e2ff6ff118712981ca82e817f28f2a85652a6@%3Cnotifications.zookeeper.apache.org%3E
h
ttps://lists.apache.org/thread.html/re41e9967bee064e7369411c28f0f5b2ad28b8334907
c9c6208017279%40%3Cnotifications.zookeeper.apache.org%3E
https://lists.apache.or
g/thread.html/re41e9967bee064e7369411c28f0f5b2ad28b8334907c9c6208017279@%3Cnotif
ications.zookeeper.apache.org%3E
https://lists.apache.org/thread.html/red3aea910
403d8620c73e1c7b9c9b145798d0469eb3298a7be7891af%40%3Cnotifications.zookeeper.apa
che.org%3E
https://lists.apache.org/thread.html/red3aea910403d8620c73e1c7b9c9b14
5798d0469eb3298a7be7891af@%3Cnotifications.zookeeper.apache.org%3E
https://lists
.apache.org/thread.html/rfa2f08b7c0caf80ca9f4a18bd875918fdd4e894e2ea47942a4589b9
c%40%3Cdev.creadur.apache.org%3E
https://lists.apache.org/thread.html/rfa2f08b7c
0caf80ca9f4a18bd875918fdd4e894e2ea47942a4589b9c@%3Cdev.creadur.apache.org%3E
htt

Vulnerability Report

ps://lists.apache.org/thread.html/rfcd2c649c205f12b72dde044f905903460669a220a2eb
7e12652d19d%40%3Cdev.zookeeper.apache.org%3E
https://lists.apache.org/thread.htm
l/rfcd2c649c205f12b72dde044f905903460669a220a2eb7e12652d19d@%3Cdev.zookeeper.apa
che.org%3E
https://lists.apache.org/thread.html/rfd01af05babc95b8949e6d8ea78d983
4699e1b06981040dde419a330%40%3Cdev.commons.apache.org%3E
https://lists.apache.or
g/thread.html/rfd01af05babc95b8949e6d8ea78d9834699e1b06981040dde419a330@%3Cdev.c
ommons.apache.org%3E
https://lists.debian.org/debian-lts-announce/2021/08/msg000
16.html
https://nvd.nist.gov/vuln/detail/CVE-2021-29425
https://security.netapp.
com/advisory/ntap-20220210-0004
https://security.netapp.com/advisory/ntap-202202
10-0004/
https://ubuntu.com/security/notices/USN-5095-1
https://www.cve.org/CVER
ecord?id=CVE-2021-29425
https://www.openwall.com/lists/oss-security/2021/04/12/1
https://www.oracle.com/security-alerts/cpuapr2022.html
https://www.oracle.com/s
ecurity-alerts/cpujan2022.html
https://www.oracle.com/security-alerts/cpujul2022
.html
https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-27807
Title:	pdfbox: infinite loop while loading a crafted PDF file
Package:	org.apache.pdfbox:pdfbox
Package ID:	org.apache.pdfbox:pdfbox:2.0.22
Installed Version:	2.0.22
Fixed Version:	2.0.23
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.5
CWE:	CWE-834
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-27807
Description:	A carefully crafted PDF file can trigger an infinite loop while loading the file . This issue affects Apache PDFBox version 2.0.22 and prior 2.0.x versions.

Vulnerability Report

http://www.openwall.com/lists/oss-security/2021/03/19/9

https://access.redhat.co

m/security/cve/CVE-2021-27807

https://github.com/apache/pdfbox

https://github.co

m/apache/pdfbox/commit/5c5a837140fbb4ef78bb5ef9f29ad537c872c83e

https://issues.a

pache.org/jira/browse/PDFBOX-4892

https://lists.apache.org/thread.html/r043edc5d

cf9199f7f882ed7906b41cb816753766e88b8792dbf319a9%40%3Cannounce.apache.org%3E

htt

ps://lists.apache.org/thread.html/r043edc5dcf9199f7f882ed7906b41cb816753766e88b8

792dbf319a9@%3Cannounce.apache.org%3E

https://lists.apache.org/thread.html/r1218

e60c32829f76943ecaca79237120c2ec1ab266459d711a578b50%40%3Cdev.pdfbox.apache.org%

3E

https://lists.apache.org/thread.html/r1218e60c32829f76943ecaca79237120c2ec1ab

266459d711a578b50@%3Cdev.pdfbox.apache.org%3E

https://lists.apache.org/thread.ht

ml/r1d268642f8b52456ee8f876b888b8ed7a9e9568c7770789f3ded7f9e%40%3Ccommits.ofbiz.

apache.org%3E

https://lists.apache.org/thread.html/r1d268642f8b52456ee8f876b888b

Vulnerability Report

8ed7a9e9568c7770789f3ded7f9e@%3Ccommits.ofbiz.apache.org%3E
https://lists.apache
.org/thread.html/r4717f902f8bc36d47b3fa978552a25e4ed3ddc2fffb52b94fbc4ab36%40%3C
users.pdfbox.apache.org%3E
https://lists.apache.org/thread.html/r4717f902f8bc36d
47b3fa978552a25e4ed3ddc2fffb52b94fbc4ab36@%3Cusers.pdfbox.apache.org%3E
https://
lists.apache.org/thread.html/r4cbc3f6981cd0a1a482531df9d44e4c42a7f63342a7ba78b7b
ff8a1b%40%3Cnotifications.james.apache.org%3E
https://lists.apache.org/thread.ht
ml/r4cbc3f6981cd0a1a482531df9d44e4c42a7f63342a7ba78b7bff8a1b@%3Cnotifications.ja
mes.apache.org%3E
https://lists.apache.org/thread.html/r54594251369e14c185da9662
a5340a52afbbdf75d61c9c3a69c8f2e8%40%3Cdev.pdfbox.apache.org%3E
https://lists.apa
che.org/thread.html/r54594251369e14c185da9662a5340a52afbbdf75d61c9c3a69c8f2e8@%3
Cdev.pdfbox.apache.org%3E
https://lists.apache.org/thread.html/r5c8e2125d18af184
c80f7a986fbe47eaf0d30457cd450133adc235ac%40%3Ccommits.ofbiz.apache.org%3E
https:
//lists.apache.org/thread.html/r5c8e2125d18af184c80f7a986fbe47eaf0d30457cd450133
adc235ac@%3Ccommits.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/r6e
067a6d83ccb6892d0ff867bd216704f21fb0b6a854dea34be04f12%40%3Cnotifications.ofbiz.
apache.org%3E
https://lists.apache.org/thread.html/r6e067a6d83ccb6892d0ff867bd21
6704f21fb0b6a854dea34be04f12@%3Cnotifications.ofbiz.apache.org%3E
https://lists.
apache.org/thread.html/r7ee634c21816c69ce829d0c41f35afa2a53a99bdd3c7cce8644fdc0e
%40%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/r7e
e634c21816c69ce829d0c41f35afa2a53a99bdd3c7cce8644fdc0e@%3Cnotifications.ofbiz.ap
ache.org%3E
https://lists.apache.org/thread.html/r818058ff1e4b9f6bef4e5a2e74faff
38cb3d3885c1e2db398bc55cfb%40%3Cusers.pdfbox.apache.org%3E
https://lists.apache.
org/thread.html/r818058ff1e4b9f6bef4e5a2e74faff38cb3d3885c1e2db398bc55cfb@%3Cuse

Vulnerability Report

rs.pdfbox.apache.org%3E
https://lists.apache.org/thread.html/r9ffe179385637b0b5c
bdabd0246118005b4b8232909d2d14cd68ccd3%40%3Ccommits.ofbiz.apache.org%3E
https://
lists.apache.org/thread.html/r9ffe179385637b0b5cbdabd0246118005b4b8232909d2d14cd
68ccd3@%3Ccommits.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/raa35
746227f3f8d50fff1db9899524423a718f6f35cd39bd4769fa6c%40%3Cnotifications.ofbiz.ap
ache.org%3E
https://lists.apache.org/thread.html/raa35746227f3f8d50fff1db9899524
423a718f6f35cd39bd4769fa6c@%3Cnotifications.ofbiz.apache.org%3E
https://lists.ap
ache.org/thread.html/rc69140d894c6a9c67a8097a25656cce59b46a5620c354ceba10543c3%4
0%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/rc691
40d894c6a9c67a8097a25656cce59b46a5620c354ceba10543c3@%3Cnotifications.ofbiz.apac
he.org%3E
https://lists.apache.org/thread.html/re1e35881482e07dc2be6058d9b444834
57f36133cac67956686ad9b9%40%3Cnotifications.ofbiz.apache.org%3E
https://lists.ap
ache.org/thread.html/re1e35881482e07dc2be6058d9b44483457f36133cac67956686ad9b9@%
3Cnotifications.ofbiz.apache.org%3E
https://lists.fedoraproject.org/archives/lis
t/package-announce%40lists.fedoraproject.org/message/2AVLKAHFMPH72TTP25INPZPGX5F
ODK3H/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fe
doraproject.org/message/6KDA2U4KL2N3XT3PM4ZJEBBA6JJIH2G4/
https://lists.fedorapr
oject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6PT72
QOFDXLJ7PLTN66EMG5EHPTE7TFZ/
https://lists.fedoraproject.org/archives/list/packa
ge-announce@lists.fedoraproject.org/message/2AVLKAHFMPH72TTP25INPZPGX5FODK3H
htt
ps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.
org/message/6KDA2U4KL2N3XT3PM4ZJEBBA6JJIH2G4
https://lists.fedoraproject.org/arc
hives/list/package-announce@lists.fedoraproject.org/message/6PT72QOFDXLJ7PLTN66E

Vulnerability Report

MG5EHPTE7TFZ
https://nvd.nist.gov/vuln/detail/CVE-2021-27807
https://svn.apache.
org/viewvc?view=revision&revision=1886911
https://www.cve.org/CVERecord?id=CVE-2
021-27807
https://www.oracle.com//security-alerts/cpujul2021.html
https://www.or
acle.com/security-alerts/cpuapr2022.html
https://www.oracle.com/security-alerts/
cpuoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-27906
Title:	pdfbox: OutOfMemory-Exception while loading a crafted PDF file
Package:	org.apache.pdfbox:pdfbox
Package ID:	org.apache.pdfbox:pdfbox:2.0.22
Installed Version:	2.0.22
Fixed Version:	2.0.23
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.5
CWE:	CWE-789
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-27906
Description:	A carefully crafted PDF file can trigger an OutOfMemory-Exception while loading the file. This issue affects Apache PDFBox version 2.0.22 and prior 2.0.x versions.

Vulnerability Report

http://www.openwall.com/lists/oss-security/2021/03/19/10

https://access.redhat.c

om/security/cve/CVE-2021-27906

https://github.com/apache/pdfbox

https://github.c

om/apache/pdfbox/commit/8c47be1011c11dc47300faecffd8ab32fba3646f

https://issues.

apache.org/jira/browse/PDFBOX-5112

https://lists.apache.org/thread.html/r1218e60

c32829f76943ecaca79237120c2ec1ab266459d711a578b50%40%3Cdev.pdfbox.apache.org%3E

https://lists.apache.org/thread.html/r1218e60c32829f76943ecaca79237120c2ec1ab266

459d711a578b50@%3Cdev.pdfbox.apache.org%3E

https://lists.apache.org/thread.html/

r1d268642f8b52456ee8f876b888b8ed7a9e9568c7770789f3ded7f9e%40%3Ccommits.ofbiz.apa

che.org%3E

https://lists.apache.org/thread.html/r1d268642f8b52456ee8f876b888b8ed

7a9e9568c7770789f3ded7f9e@%3Ccommits.ofbiz.apache.org%3E

https://lists.apache.or

g/thread.html/r4cbc3f6981cd0a1a482531df9d44e4c42a7f63342a7ba78b7bff8a1b%40%3Cnot

ifications.james.apache.org%3E

Vulnerability Report

https://lists.apache.org/thread.html/r4cbc3f6981c
d0a1a482531df9d44e4c42a7f63342a7ba78b7bff8a1b@%3Cnotifications.james.apache.org%
3E
https://lists.apache.org/thread.html/r54594251369e14c185da9662a5340a52afbbdf7
5d61c9c3a69c8f2e8%40%3Cdev.pdfbox.apache.org%3E
https://lists.apache.org/thread.
html/r54594251369e14c185da9662a5340a52afbbdf75d61c9c3a69c8f2e8@%3Cdev.pdfbox.apa
che.org%3E
https://lists.apache.org/thread.html/r5c8e2125d18af184c80f7a986fbe47e
af0d30457cd450133adc235ac%40%3Ccommits.ofbiz.apache.org%3E
https://lists.apache.
org/thread.html/r5c8e2125d18af184c80f7a986fbe47eaf0d30457cd450133adc235ac@%3Ccom
mits.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/r64982b768c8a2220b
07aaf813bd099a9863de0d13eb212fd4efe208f%40%3Cusers.pdfbox.apache.org%3E
https://
lists.apache.org/thread.html/r64982b768c8a2220b07aaf813bd099a9863de0d13eb212fd4e
fe208f@%3Cusers.pdfbox.apache.org%3E
https://lists.apache.org/thread.html/r6e067
a6d83ccb6892d0ff867bd216704f21fb0b6a854dea34be04f12%40%3Cnotifications.ofbiz.apa
che.org%3E
https://lists.apache.org/thread.html/r6e067a6d83ccb6892d0ff867bd21670
4f21fb0b6a854dea34be04f12@%3Cnotifications.ofbiz.apache.org%3E
https://lists.apa
che.org/thread.html/r7ee634c21816c69ce829d0c41f35afa2a53a99bdd3c7cce8644fdc0e%40
%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/r7ee63
4c21816c69ce829d0c41f35afa2a53a99bdd3c7cce8644fdc0e@%3Cnotifications.ofbiz.apach
e.org%3E
https://lists.apache.org/thread.html/r9ffe179385637b0b5cbdabd0246118005
b4b8232909d2d14cd68ccd3%40%3Ccommits.ofbiz.apache.org%3E
https://lists.apache.or
g/thread.html/r9ffe179385637b0b5cbdabd0246118005b4b8232909d2d14cd68ccd3@%3Ccommi
ts.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/raa35746227f3f8d50ff
f1db9899524423a718f6f35cd39bd4769fa6c%40%3Cnotifications.ofbiz.apache.org%3E
htt

Vulnerability Report

ps://lists.apache.org/thread.html/raa35746227f3f8d50fff1db9899524423a718f6f35cd3
9bd4769fa6c@%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache.org/thread
.html/rc69140d894c6a9c67a8097a25656cce59b46a5620c354ceba10543c3%40%3Cnotificatio
ns.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/rc69140d894c6a9c67a8
097a25656cce59b46a5620c354ceba10543c3@%3Cnotifications.ofbiz.apache.org%3E
https
://lists.apache.org/thread.html/rdf78aef4793362e778e21e34328b0456e302bde4b7e74f2
29df0ee04%40%3Cannounce.apache.org%3E
https://lists.apache.org/thread.html/rdf78
aef4793362e778e21e34328b0456e302bde4b7e74f229df0ee04@%3Cannounce.apache.org%3E
h
ttps://lists.apache.org/thread.html/re1e35881482e07dc2be6058d9b44483457f36133cac
67956686ad9b9%40%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache.org/th
read.html/re1e35881482e07dc2be6058d9b44483457f36133cac67956686ad9b9@%3Cnotificat
ions.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/rf35026148ccc0e1af
133501c0d003d052883fcc65107b3ff5d3b61cd%40%3Cusers.pdfbox.apache.org%3E
https://
lists.apache.org/thread.html/rf35026148ccc0e1af133501c0d003d052883fcc65107b3ff5d
3b61cd@%3Cusers.pdfbox.apache.org%3E
https://lists.fedoraproject.org/archives/li
st/package-announce%40lists.fedoraproject.org/message/2AVLKAHFMPH72TTP25INPZPGX5
FODK3H/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.f
edoraproject.org/message/6KDA2U4KL2N3XT3PM4ZJEBBA6JJIH2G4/
https://lists.fedorap
roject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6PT7
2QOFDXLJ7PLTN66EMG5EHPTE7TFZ/
https://lists.fedoraproject.org/archives/list/pack
age-announce@lists.fedoraproject.org/message/2AVLKAHFMPH72TTP25INPZPGX5FODK3H
ht
tps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject
.org/message/6KDA2U4KL2N3XT3PM4ZJEBBA6JJIH2G4
https://lists.fedoraproject.org/ar

Vulnerability Report

chives/list/package-announce@lists.fedoraproject.org/message/6PT72QOFDXLJ7PLTN66
EMG5EHPTE7TFZ
https://nvd.nist.gov/vuln/detail/CVE-2021-27906
https://www.cve.or
g/CVERecord?id=CVE-2021-27906
https://www.oracle.com//security-alerts/cpujul2021
.html
https://www.oracle.com/security-alerts/cpuapr2022.html
https://www.oracle.
com/security-alerts/cpuoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-31811
Title:	pdfbox: OutOfMemory-Exception while loading a crafted PDF file
Package:	org.apache.pdfbox:pdfbox
Package ID:	org.apache.pdfbox:pdfbox:2.0.22
Installed Version:	2.0.22
Fixed Version:	2.0.24
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.5
CWE:	CWE-789, CWE-770
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-31811
Description:	In Apache PDFBox, a carefully crafted PDF file can trigger an OutOfMemory-Except ion while loading the file. This issue affects Apache PDFBox version 2.0.23 and prior 2.0.x versions.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2021/06/12/2 https://access.redhat.co m/security/cve/CVE-2021-31811 https://lists.apache.org/thread.html/r132e9dbbe0eb dc08b39583d8be0a575fdba573d60a42d940228bceff%40%3Cnotifications.ofbiz.apache.org %3E https://lists.apache.org/thread.html/r132e9dbbe0ebdc08b39583d8be0a575fdba573 d60a42d940228bceff@%3Cnotifications.ofbiz.apache.org%3E https://lists.apache.org /thread.html/r143fd8445e0e778f4a85187bd79438630b96b8040e9401751fdb8aea%40%3Ccomm its.ofbiz.apache.org%3E https://lists.apache.org/thread.html/r143fd8445e0e778f4a 85187bd79438630b96b8040e9401751fdb8aea@%3Ccommits.ofbiz.apache.org%3E https://li sts.apache.org/thread.html/r179cc3b6822c167702ab35fe36093d5da4c99af44238c8a754c6 860f%40%3Ccommits.ofbiz.apache.org%3E https://lists.apache.org/thread.html/r179c c3b6822c167702ab35fe36093d5da4c99af44238c8a754c6860f@%3Ccommits.ofbiz.apache.org %3E https://lists.apache.org/thread.html/r2090789e4dcc2c87aacbd87d5f18e2d64dcb9f 6eb7c47f5cf7d293cb%40%3Cnotifications.ofbiz.apache.org%3E

Vulnerability Report

https://lists.apache.o
rg/thread.html/r2090789e4dcc2c87aacbd87d5f18e2d64dcb9f6eb7c47f5cf7d293cb@%3Cnoti
fications.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/rd4b6db6c3b8a
b3c70f1c3bbd725a40920896453ffc2744ade6afd9fb%40%3Cnotifications.ofbiz.apache.org
%3E
https://lists.apache.org/thread.html/rd4b6db6c3b8ab3c70f1c3bbd725a4092089645
3ffc2744ade6afd9fb@%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache.org
/thread.html/re0cacd3fb337cdf8469853913ed2b4ddd8f8bfc52ff0ddbe61c1dfba%40%3Ccomm
its.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/re0cacd3fb337cdf846
9853913ed2b4ddd8f8bfc52ff0ddbe61c1dfba@%3Ccommits.ofbiz.apache.org%3E
https://li
sts.apache.org/thread.html/re3bd16f0cc8f1fbda46b06a4b8241cd417f71402809baa81548f
c20e%40%3Cusers.pdfbox.apache.org%3E
https://lists.apache.org/thread.html/re3bd1
6f0cc8f1fbda46b06a4b8241cd417f71402809baa81548fc20e@%3Cusers.pdfbox.apache.org%3
E
https://lists.apache.org/thread.html/rf937c2236e6c79cdb99f76a70690dd345e53dbe0
707cb506a202e43e%40%3Cannounce.apache.org%3E
https://lists.apache.org/thread.htm
l/rf937c2236e6c79cdb99f76a70690dd345e53dbe0707cb506a202e43e@%3Cannounce.apache.o
rg%3E
https://lists.apache.org/thread.html/rfe26bcaba564deb505c32711ba68df7ec589
797dcd96ff3389a8aaba%40%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache
.org/thread.html/rfe26bcaba564deb505c32711ba68df7ec589797dcd96ff3389a8aaba@%3Cno
tifications.ofbiz.apache.org%3E
https://lists.fedoraproject.org/archives/list/pa
ckage-announce%40lists.fedoraproject.org/message/7HHWJRFXZ3PTKLJCOM7WJEYZFKFWMNS
V/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedora
project.org/message/MDJKJQOMVFDFIDS27OQJXNOYHV2O273D/
https://lists.fedoraprojec
t.org/archives/list/package-announce@lists.fedoraproject.org/message/7HHWJRFXZ3P
TKLJCOM7WJEYZFKFWMNSV

Vulnerability Report

https://lists.fedoraproject.org/archives/list/package-anno
unce@lists.fedoraproject.org/message/MDJKJQOMVFDFIDS27OQJXNOYHV2O273D
https://nv
d.nist.gov/vuln/detail/CVE-2021-31811
https://www.cve.org/CVERecord?id=CVE-2021-
31811
https://www.oracle.com//security-alerts/cpujul2021.html
https://www.oracle
.com/security-alerts/cpuapr2022.html
https://www.oracle.com/security-alerts/cpuj
an2022.html
https://www.oracle.com/security-alerts/cpujul2022.html
https://www.o
racle.com/security-alerts/cpuoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2021-31812
Title:	pdfbox: infinite loop while loading a crafted PDF file
Package:	org.apache.pdfbox:pdfbox
Package ID:	org.apache.pdfbox:pdfbox:2.0.22
Installed Version:	2.0.22
Fixed Version:	2.0.24
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.5
CWE:	CWE-834, CWE-835
Primary URL:	https://avd.aquasec.com/nvd/cve-2021-31812
Description:	In Apache PDFBox, a carefully crafted PDF file can trigger an infinite loop whil e loading the file. This issue affects Apache PDFBox version 2.0.23 and prior 2. 0.x versions.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2021/06/12/1 https://access.redhat.co m/security/cve/CVE-2021-31812 https://lists.apache.org/thread.html/r132e9dbbe0eb dc08b39583d8be0a575fdba573d60a42d940228bceff%40%3Cnotifications.ofbiz.apache.org %3E https://lists.apache.org/thread.html/r132e9dbbe0ebdc08b39583d8be0a575fdba573 d60a42d940228bceff@%3Cnotifications.ofbiz.apache.org%3E https://lists.apache.org /thread.html/r143fd8445e0e778f4a85187bd79438630b96b8040e9401751fdb8aea%40%3Ccomm its.ofbiz.apache.org%3E https://lists.apache.org/thread.html/r143fd8445e0e778f4a 85187bd79438630b96b8040e9401751fdb8aea@%3Ccommits.ofbiz.apache.org%3E https://li sts.apache.org/thread.html/r179cc3b6822c167702ab35fe36093d5da4c99af44238c8a754c6 860f%40%3Ccommits.ofbiz.apache.org%3E https://lists.apache.org/thread.html/r179c c3b6822c167702ab35fe36093d5da4c99af44238c8a754c6860f@%3Ccommits.ofbiz.apache.org %3E https://lists.apache.org/thread.html/r2090789e4dcc2c87aacbd87d5f18e2d64dcb9f 6eb7c47f5cf7d293cb%40%3Cnotifications.ofbiz.apache.org%3E

Vulnerability Report

https://lists.apache.o
rg/thread.html/r2090789e4dcc2c87aacbd87d5f18e2d64dcb9f6eb7c47f5cf7d293cb@%3Cnoti
fications.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/ra2ab0ce69ce8
aaff0773b8c1036438387ce004c2afc6f066626e205e%40%3Cusers.pdfbox.apache.org%3E
htt
ps://lists.apache.org/thread.html/ra2ab0ce69ce8aaff0773b8c1036438387ce004c2afc6f
066626e205e@%3Cusers.pdfbox.apache.org%3E
https://lists.apache.org/thread.html/r
d4b6db6c3b8ab3c70f1c3bbd725a40920896453ffc2744ade6afd9fb%40%3Cnotifications.ofbi
z.apache.org%3E
https://lists.apache.org/thread.html/rd4b6db6c3b8ab3c70f1c3bbd72
5a40920896453ffc2744ade6afd9fb@%3Cnotifications.ofbiz.apache.org%3E
https://list
s.apache.org/thread.html/re0cacd3fb337cdf8469853913ed2b4ddd8f8bfc52ff0ddbe61c1df
ba%40%3Ccommits.ofbiz.apache.org%3E
https://lists.apache.org/thread.html/re0cacd
3fb337cdf8469853913ed2b4ddd8f8bfc52ff0ddbe61c1dfba@%3Ccommits.ofbiz.apache.org%3
E
https://lists.apache.org/thread.html/rf251f6c358087107f8c23473468b279d59d50a75
db6b4768165c78d3%40%3Cannounce.apache.org%3E
https://lists.apache.org/thread.htm
l/rf251f6c358087107f8c23473468b279d59d50a75db6b4768165c78d3@%3Cannounce.apache.o
rg%3E
https://lists.apache.org/thread.html/rfe26bcaba564deb505c32711ba68df7ec589
797dcd96ff3389a8aaba%40%3Cnotifications.ofbiz.apache.org%3E
https://lists.apache
.org/thread.html/rfe26bcaba564deb505c32711ba68df7ec589797dcd96ff3389a8aaba@%3Cno
tifications.ofbiz.apache.org%3E
https://lists.fedoraproject.org/archives/list/pa
ckage-announce%40lists.fedoraproject.org/message/7HHWJRFXZ3PTKLJCOM7WJEYZFKFWMNS
V/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedora
project.org/message/MDJKJQOMVFDFIDS27OQJXNOYHV2O273D/
https://lists.fedoraprojec
t.org/archives/list/package-announce@lists.fedoraproject.org/message/7HHWJRFXZ3P
TKLJCOM7WJEYZFKFWMNSV

Vulnerability Report

https://lists.fedoraproject.org/archives/list/package-anno
unce@lists.fedoraproject.org/message/MDJKJQOMVFDFIDS27OQJXNOYHV2O273D
https://nv
d.nist.gov/vuln/detail/CVE-2021-31812
https://www.cve.org/CVERecord?id=CVE-2021-
31812
https://www.oracle.com/security-alerts/cpuapr2022.html
https://www.oracle.
com/security-alerts/cpujan2022.html
https://www.oracle.com/security-alerts/cpuju
l2022.html
https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2017-5644
Title:	Apache POI in versions prior to release 3.15 allows remote attackers t ...
Package:	org.apache.poi:poi
Package ID:	org.apache.poi:poi:3.13
Installed Version:	3.13
Fixed Version:	3.15
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.5
CWE:	CWE-776
Primary URL:	https://avd.aquasec.com/nvd/cve-2017-5644
Description:	Apache POI in versions prior to release 3.15 allows remote attackers to cause a denial of service (CPU consumption) via a specially crafted OOXML file, aka an X ML Entity Expansion (XEE) attack.
References:	http://poi.apache.org/#20+March+2017+-+CVE-2017-5644+-+Possible+DOS+%28Denial+of +Service%29+in+Apache+POI+versions+prior+to+3.15 http://www.securityfocus.com/bi d/96983 https://nvd.nist.gov/vuln/detail/CVE-2017-5644 https://www.oracle.com/se curity-alerts/cpuoct2020.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2019-12415
Title:	poi: a specially crafted Microsoft Excel document allows attacker to read files from the local filesystem
Package:	org.apache.poi:poi
Package ID:	org.apache.poi:poi:3.13
Installed Version:	3.13
Fixed Version:	4.1.1
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.5
CWE:	CWE-611
Primary URL:	https://avd.aquasec.com/nvd/cve-2019-12415
Description:	In Apache POI up to 4.1.0, when using the tool XSSFExportToXml to convert user-provided Microsoft Excel documents, a specially crafted document can allow an attacker to read files from the local filesystem or from internal network resources via XML External Entity (XXE) Processing.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2019-12415 https://github.com/apache/ poi https://lists.apache.org/thread.html/13a54b6a03369cfb418a699180ffb83bd727320 b6ddfec198b9b728e%40%3Cannounce.apache.org%3E https://lists.apache.org/thread.ht ml/13a54b6a03369cfb418a699180ffb83bd727320b6ddfec198b9b728e@%3Cannounce.apache.o rg%3E https://lists.apache.org/thread.html/2ac0327748de0c2b3c1c012481b79936797c7 11724e0b7da83cf564c%40%3Cuser.tika.apache.org%3E https://lists.apache.org/thread .html/2ac0327748de0c2b3c1c012481b79936797c711724e0b7da83cf564c@%3Cuser.tika.apac he.org%3E https://lists.apache.org/thread.html/895164e03a3c327449069e2fd6ced0367 561878b3ae6a8ec740c2007%40%3Cuser.tika.apache.org%3E https://lists.apache.org/th read.html/895164e03a3c327449069e2fd6ced0367561878b3ae6a8ec740c2007@%3Cuser.tika. apache.org%3E https://lists.apache.org/thread.html/d88b8823867033514d7ec05d66f88

Vulnerability Report

c70dc207604d3dcbd44fd88464c%40%3Cuser.tika.apache.org%3E
https://lists.apache.or
g/thread.html/d88b8823867033514d7ec05d66f88c70dc207604d3dcbd44fd88464c@%3Cuser.t
ika.apache.org%3E
https://lists.apache.org/thread.html/r204ba2a9ea750f38d789d2bb
429cc0925ad6133deea7cbc3001d96b5%40%3Csolr-user.lucene.apache.org%3E
https://lis
ts.apache.org/thread.html/r204ba2a9ea750f38d789d2bb429cc0925ad6133deea7cbc3001d9
6b5@%3Csolr-user.lucene.apache.org%3E
https://nvd.nist.gov/vuln/detail/CVE-2019-
12415
https://www.cve.org/CVERecord?id=CVE-2019-12415
https://www.oracle.com//se
curity-alerts/cpujul2021.html
https://www.oracle.com/security-alerts/cpuApr2021.
html
https://www.oracle.com/security-alerts/cpuapr2020.html
https://www.oracle.c
om/security-alerts/cpujan2020.html
https://www.oracle.com/security-alerts/cpujan
2021.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.ora
cle.com/security-alerts/cpuoct2020.html
https://www.oracle.com/security-alerts/c
puoct2021.html

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2025-31672
Title:	org.apache.poi/poi-ooxml: Apache POI: parsing OOXML based files (xlsx, docx, etc .), poi-ooxml could read unexpected data if underlying zip has duplicate zip entry names
Package:	org.apache.poi:poi-ooxml
Package ID:	org.apache.poi:poi-ooxml:3.13
Installed Version:	3.13
Fixed Version:	5.4.0
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	CWE-20
Primary URL:	https://avd.aquasec.com/nvd/cve-2025-31672
Description:	Improper Input Validation vulnerability in Apache POI. The issue affects the parsing of OOXML format files like xlsx, docx and pptx. These file formats are basically zip files and it is possible for malicious users to add zip entries with duplicate names (including the path) in the zip. In this case, products reading the affected file could read different data because 1 of the zip entries with the duplicate name is selected over another but different products may choose a different zip entry. This issue affects Apache POI poi-ooxml before 5.4.0. poi-ooxml 5.4.0 has a check that throws an exception if zip entries with duplicate file names are found in the input file. Users are recommended to upgrade to version poi-ooxml 5.4.0, which fixes the issue. Please read https://poi.apache.org/security.html for recommendations about how to use the POI libraries securely.

Vulnerability Report

References:

http://www.openwall.com/lists/oss-security/2025/04/08/2

https://access.redhat.co

m/security/cve/CVE-2025-31672

https://bz.apache.org/bugzilla/show_bug.cgi?id=696

20

https://github.com/apache/poi

https://lists.apache.org/thread/k14w8vcjqy4h34h

h5kzldko78kpylkq5

https://nvd.nist.gov/vuln/detail/CVE-2025-31672

Vulnerability Report

https://www.cv
e.org/CVERecord?id=CVE-2025-31672

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2012-1007
Title:	struts: multiple XSS flaws
Package:	org.apache.struts:struts-core
Package ID:	org.apache.struts:struts-core:1.3.8
Installed Version:	1.3.8
Fixed Version:	N/A
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	N/A
CWE:	CWE-79
Primary URL:	https://avd.aquasec.com/nvd/cve-2012-1007
Description:	Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 1.3.10 allo w remote attackers to inject arbitrary web script or HTML via (1) the name param eter to struts-examples/upload/upload-submit.do, or the message parameter to (2) struts-cookbook/processSimple.do or (3) struts-cookbook/processDyna.do.
References:	http://secpod.org/advisories/SecPod_Apache_Struts_Multiple_Parsistant_XSS_Vulns. txt http://secpod.org/blog/?p=450 http://www.oracle.com/technetwork/security-adv isory/cpuoct2016-2881722.html http://www.oracle.com/technetwork/security-advisor y/cpuoct2018-4428296.html http://www.securityfocus.com/bid/51900 https://access. redhat.com/security/cve/CVE-2012-1007 https://exchange.xforce.ibmcloud.com/vulne rabilities/73052 https://nvd.nist.gov/vuln/detail/CVE-2012-1007 https://www.cve. org/CVERecord?id=CVE-2012-1007

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-41080
Title:	tomcat: Open Redirect vulnerability in FORM authentication
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	8.5.93, 9.0.80, 10.1.13, 11.0.0-M11
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.1
CWE:	CWE-601
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-41080
Description:	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authen tication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92. The vulnerability is limited to the ROOT (defau lt) web application.

Vulnerability Report

References:	https://access.redhat.com/errata/RHSA-2024:0474 https://access.redhat.com/securi ty/cve/CVE-2023-41080 https://bugzilla.redhat.com/2235370 https://bugzilla.redha t.com/2243749 https://bugzilla.redhat.com/2243751 https://bugzilla.redhat.com/22 43752 https://errata.almalinux.org/9/ALSA-2024-0474.html https://github.com/apac he/tomcat https://github.com/apache/tomcat/commit/4998ad745b67edeadefe541c94ed02 9b53933d3b https://github.com/apache/tomcat/commit/77c0ce2d169efa248b64b992e547a ad549ec906b https://github.com/apache/tomcat/commit/77c0ce2d169efa248b64b992e547

Vulnerability Report

aad549ec906b (9.0.80)
https://github.com/apache/tomcat/commit/bb4624a9f3e69d4951
82ebfa68d7983076407a27
https://github.com/apache/tomcat/commit/bb4624a9f3e69d495
182ebfa68d7983076407a27 (10.1.13)
https://github.com/apache/tomcat/commit/e3703c
9abb8fe0d5602f6ba8a8f11d4b6940815a
https://linux.oracle.com/cve/CVE-2023-41080.h
tml
https://linux.oracle.com/errata/ELSA-2024-0474.html
https://lists.apache.org
/thread/71wvwprtx2j2m54fovq9zr7gbm2wow2f
https://lists.debian.org/debian-lts-ann
ounce/2023/10/msg00020.html
https://nvd.nist.gov/vuln/detail/CVE-2023-41080
http
s://security.netapp.com/advisory/ntap-20230921-0006
https://security.netapp.com/
advisory/ntap-20230921-0006/
https://ubuntu.com/security/notices/USN-7106-1
http
s://www.cve.org/CVERecord?id=CVE-2023-41080
https://www.debian.org/security/2023
/dsa-5521
https://www.debian.org/security/2023/dsa-5522

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-42795
Title:	tomcat: improper cleaning of recycled objects could lead to information leak
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.0-M12, 10.1.14, 9.0.81, 8.5.94
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	CWE-459
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-42795
Description:	Incomplete Cleanup vulnerability in Apache Tomcat.When recycling various interna l objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 thr ough 10.1.13, from 9.0.0-M1 through 9.0.80 and from 8.5.0 through 8.5.93, an err or could cause Tomcat to skip some parts of the recycling process leading to i nformation leaking from the current request/response to the next. Users are rec ommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwar ds or 8.5.94 onwards, which fixes the issue.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2023/10/10/9 https://access.redhat.co m/errata/RHSA-2024:0474 https://access.redhat.com/security/cve/CVE-2023-42795 ht tps://bugzilla.redhat.com/2235370 https://bugzilla.redhat.com/2243749 https://bu gzilla.redhat.com/2243751 https://bugzilla.redhat.com/2243752 https://errata.alm alinux.org/9/ALSA-2024-0474.html https://github.com/apache/tomcat

Vulnerability Report

https://github
.com/apache/tomcat/commit/30f8063d7a9b4c43ae4722f5e382a76af1d7a6bf
https://githu
b.com/apache/tomcat/commit/44d05d75d696ca10ce251e4e370511e38f20ae75
https://gith
ub.com/apache/tomcat/commit/9375d67106f8df9eb9d7b360b2bef052fe67d3d4
https://git
hub.com/apache/tomcat/commit/d6db22e411307c97ddf78315c15d5889356eca38
https://li
nux.oracle.com/cve/CVE-2023-42795.html
https://linux.oracle.com/errata/ELSA-2024
-0474.html
https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw
http
s://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
https://nvd.nist.
gov/vuln/detail/CVE-2023-42795
https://security.netapp.com/advisory/ntap-2023110
3-0007
https://security.netapp.com/advisory/ntap-20231103-0007/
https://ubuntu.c
om/security/notices/USN-7106-1
https://www.cve.org/CVERecord?id=CVE-2023-42795
h
ttps://www.debian.org/security/2023/dsa-5521
https://www.debian.org/security/202
3/dsa-5522
https://www.openwall.com/lists/oss-security/2023/10/10/9

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-44487
Title:	HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack)
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.0-M12, 10.1.14, 9.0.81, 8.5.94
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	CWE-400
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-44487
Description:	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Vulnerability Report

http://www.openwall.com/lists/oss-security/2023/10/10/6

http://www.openwall.com/

lists/oss-security/2023/10/10/7

http://www.openwall.com/lists/oss-security/2023/

10/13/4

http://www.openwall.com/lists/oss-security/2023/10/13/9

http://www.openw

all.com/lists/oss-security/2023/10/18/4

http://www.openwall.com/lists/oss-securi

ty/2023/10/18/8

http://www.openwall.com/lists/oss-security/2023/10/19/6

http://w

ww.openwall.com/lists/oss-security/2023/10/20/8

https://access.redhat.com/errata

/RHSA-2023:6746

https://access.redhat.com/security/cve/CVE-2023-44487

https://ac

cess.redhat.com/security/cve/cve-2023-44487

https://akka.io/security/akka-http-c

ve-2023-44487.html

Vulnerability Report

https://arstechnica.com/security/2023/10/how-ddosers-used-the
-http-2-protocol-to-deliver-attacks-of-unprecedented-size
https://arstechnica.co
m/security/2023/10/how-ddosers-used-the-http-2-protocol-to-deliver-attacks-of-un
precedented-size/
https://aws.amazon.com/security/security-bulletins/AWS-2023-01
1
https://aws.amazon.com/security/security-bulletins/AWS-2023-011/
https://blog.
cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack
https://blog.cl
oudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/
https://blog.clo
udflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack
https://blog.
cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/
https://b
log.litespeedtech.com/2023/10/11/rapid-reset-http-2-vulnerablilty
https://blog.l
itespeedtech.com/2023/10/11/rapid-reset-http-2-vulnerablilty/
https://blog.qualy
s.com/vulnerabilities-threat-research/2023/10/10/cve-2023-44487-http-2-rapid-res
et-attack
https://blog.vespa.ai/cve-2023-44487
https://blog.vespa.ai/cve-2023-44
487/
https://bugzilla.proxmox.com/show_bug.cgi?id=4988
https://bugzilla.redhat.c
om/2242803
https://bugzilla.redhat.com/show_bug.cgi?id=2242803
https://bugzilla.
suse.com/show_bug.cgi?id=1216123
https://cgit.freebsd.org/ports/commit/?id=c64c3
29c2c1752f46b73e3e6ce9f4329be6629f9
https://chaos.social/@icing/1112109159187805
32
https://cloud.google.com/blog/products/identity-security/google-cloud-mitigat

ed-largest-ddos-attack-peaking-above-398-million-rps
https://cloud.google.com/bl
og/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking
-above-398-million-rps/
https://cloud.google.com/blog/products/identity-security
/how-it-works-the-novel-http2-rapid-reset-ddos-attack
https://community.traefik.
io/t/is-traefik-vulnerable-to-cve-2023-44487/20125
https://cve.mitre.org/cgi-bin
/cvename.cgi?name=CVE-2023-44487
https://devblogs.microsoft.com/dotnet/october-2
023-updates/
https://discuss.hashicorp.com/t/hcsec-2023-32-vault-consul-and-boun
dary-affected-by-http-2-rapid-reset-denial-of-service-vulnerability-cve-2023-444
87/59715
https://edg.io/lp/blog/resets-leaks-ddos-and-the-tale-of-a-hidden-cve
h
ttps://errata.almalinux.org/9/ALSA-2023-6746.html
https://errata.rockylinux.org/
RLSA-2023:5838
https://forums.swift.org/t/swift-nio-http2-security-update-cve-20
23-44487-http-2-dos/67764
https://gist.github.com/adulau/7c2bfb8e9cdbe4b35a5e131
c66a0c088
https://github.com/Azure/AKS/issues/3947
https://github.com/Kong/kong/
discussions/11741
https://github.com/advisories/GHSA-qppj-fm5r-hxr3
https://gith
ub.com/advisories/GHSA-vx74-f528-fxqg
https://github.com/advisories/GHSA-xpw8-rc
wv-8f8p
https://github.com/akka/akka-http/issues/4323
https://github.com/akka/ak
ka-http/pull/4324
https://github.com/akka/akka-http/pull/4325
https://github.com

Vulnerability Report

/alibaba/tengine/issues/1872
https://github.com/apache/apisix/issues/10320
https
://github.com/apache/httpd-site/pull/10
https://github.com/apache/httpd/blob/afc
dbeebbff4b0c50ea26cdd16e178c0d1f24152/modules/http2/h2_mplx.c#L1101-L1113
https:
//github.com/apache/tomcat/commit/944332bb15bd2f3bf76ec2caeb1ff0a58a3bc628
https
://github.com/apache/tomcat/tree/main/java/org/apache/coyote/http2
https://githu
b.com/apache/trafficserver/pull/10564
https://github.com/apple/swift-nio-http2
h
ttps://github.com/apple/swift-nio-http2/security/advisories/GHSA-qppj-fm5r-hxr3
https://github.com/arkrwn/PoC/tree/main/CVE-2023-44487
https://github.com/bcdann
yboy/CVE-2023-44487
https://github.com/caddyserver/caddy/issues/5877
https://git
hub.com/caddyserver/caddy/releases/tag/v2.7.5
https://github.com/dotnet/announce
ments/issues/277
https://github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2
c1c1dec1ce9ec/release-notes/6.0/6.0.23/6.0.23.md?plain=1#L73
https://github.com/
eclipse/jetty.project/issues/10679
https://github.com/envoyproxy/envoy/pull/3005
5
https://github.com/etcd-io/etcd/issues/16740
https://github.com/facebook/proxy
gen/pull/466
https://github.com/golang/go/issues/63417
https://github.com/grpc/g
rpc-go/pull/6703
https://github.com/grpc/grpc-go/releases

Vulnerability Report

https://github.com/grp
c/grpc/releases/tag/v1.59.2
https://github.com/h2o/h2o/pull/3291
https://github.
com/h2o/h2o/security/advisories/GHSA-2m7v-gc89-fjqf
https://github.com/haproxy/h
aproxy/issues/2312
https://github.com/hyperium/hyper/issues/3337
https://github.
com/icing/mod_h2/blob/0a864782af0a942aa2ad4ed960a6b32cd35bcf0a/mod_http2/README.
md?plain=1#L239-L244
https://github.com/junkurihara/rust-rpxy/issues/97
https://
github.com/kazu-yamamoto/http2/commit/f61d41a502bd0f60eb24e1ce14edc7b6df6722a1
h
ttps://github.com/kazu-yamamoto/http2/issues/93
https://github.com/kubernetes/ku
bernetes/pull/121120
https://github.com/line/armeria/pull/5232
https://github.co
m/linkerd/website/pull/1695/commits/4b9c6836471bc8270ab48aae6fd2181bc73fd632
htt
ps://github.com/micrictor/http2-rst-stream
https://github.com/microsoft/CBL-Mari
ner/pull/6381
https://github.com/netty/netty/commit/58f75f665aa81a8cbcf6ffa74820
042a285c5e61
https://github.com/nghttp2/nghttp2/pull/1961
https://github.com/ngh
ttp2/nghttp2/releases/tag/v1.57.0
https://github.com/ninenines/cowboy/issues/161
5
https://github.com/nodejs/node/pull/50121
https://github.com/openresty/openres
ty/issues/930
https://github.com/opensearch-project/data-prepper/issues/3474
htt

ps://github.com/oqtane/oqtane.framework/discussions/3367
https://github.com/proj
ectcontour/contour/pull/5826
https://github.com/tempesta-tech/tempesta/issues/19
86
https://github.com/varnishcache/varnish-cache/issues/3996
https://go.dev/cl/5
34215
https://go.dev/cl/534235
https://go.dev/issue/63417
https://groups.google.
com/g/golang-announce/c/iNNxDTCjZvo
https://groups.google.com/g/golang-announce/
c/iNNxDTCjZvo/m/UDd7VKQuAAAJ
https://istio.io/latest/news/security/istio-securit
y-2023-004
https://istio.io/latest/news/security/istio-security-2023-004/
https:
//linkerd.io/2023/10/12/linkerd-cve-2023-44487
https://linkerd.io/2023/10/12/lin
kerd-cve-2023-44487/
https://linux.oracle.com/cve/CVE-2023-44487.html
https://li
nux.oracle.com/errata/ELSA-2024-1444.html
https://lists.apache.org/thread/5py8h4
2mxfsn8l1wy6o41xwhsjlsd87q
https://lists.debian.org/debian-lts-announce/2023/10/
msg00020.html
https://lists.debian.org/debian-lts-announce/2023/10/msg00023.html
https://lists.debian.org/debian-lts-announce/2023/10/msg00024.html
https://list
s.debian.org/debian-lts-announce/2023/10/msg00045.html
https://lists.debian.org/
debian-lts-announce/2023/10/msg00047.html
https://lists.debian.org/debian-lts-an
nounce/2023/11/msg00001.html

Vulnerability Report

https://lists.debian.org/debian-lts-announce/2023/1
1/msg00012.html
https://lists.fedoraproject.org/archives/list/package-announce%4
0lists.fedoraproject.org/message/2MBEPPC36UBVOZZNAXFHKLFGSLCMN5LI
https://lists.
fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/messa
ge/2MBEPPC36UBVOZZNAXFHKLFGSLCMN5LI/
https://lists.fedoraproject.org/archives/li
st/package-announce%40lists.fedoraproject.org/message/3N4NJ7FR4X4FPZUGNTQAPSTVB2
HB2Y4A
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fe
doraproject.org/message/3N4NJ7FR4X4FPZUGNTQAPSTVB2HB2Y4A/
https://lists.fedorapr
oject.org/archives/list/package-announce%40lists.fedoraproject.org/message/BFQD3
KUEMFBHPAPBGLWQC34L4OWL5HAZ
https://lists.fedoraproject.org/archives/list/packag
e-announce%40lists.fedoraproject.org/message/BFQD3KUEMFBHPAPBGLWQC34L4OWL5HAZ/
h
ttps://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproj
ect.org/message/CLB4TW7KALB3EEQWNWCN7OUIWWVWWCG2
https://lists.fedoraproject.org
/archives/list/package-announce%40lists.fedoraproject.org/message/CLB4TW7KALB3EE
QWNWCN7OUIWWVWWCG2/
https://lists.fedoraproject.org/archives/list/package-announ
ce%40lists.fedoraproject.org/message/E72T67UPDRXHIDLO3OROR25YAMN4GGW5
https://li
sts.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/m
essage/E72T67UPDRXHIDLO3OROR25YAMN4GGW5/
https://lists.fedoraproject.org/archive
s/list/package-announce%40lists.fedoraproject.org/message/FNA62Q767CFAFHBCDKYNPB
MZWB7TWYVU
https://lists.fedoraproject.org/archives/list/package-announce%40list
s.fedoraproject.org/message/FNA62Q767CFAFHBCDKYNPBMZWB7TWYVU/
https://lists.fedo
raproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H
T7T2R4MQKLIF4ODV4BDLPARWFPCJ5CZ
https://lists.fedoraproject.org/archives/list/pa

ckage-announce%40lists.fedoraproject.org/message/HT7T2R4MQKLIF4ODV4BDLPARWFPCJ5C
Z/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedora
project.org/message/JIZSEFC3YKCGABA2BZW6ZJRMDZJMB7PJ
https://lists.fedoraproject
.org/archives/list/package-announce%40lists.fedoraproject.org/message/JIZSEFC3YK
CGABA2BZW6ZJRMDZJMB7PJ/
https://lists.fedoraproject.org/archives/list/package-an
nounce%40lists.fedoraproject.org/message/JMEXY22BFG5Q64HQCM5CK2Q7KDKVV4TY
https:
//lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.o
rg/message/JMEXY22BFG5Q64HQCM5CK2Q7KDKVV4TY/
https://lists.fedoraproject.org/arc
hives/list/package-announce%40lists.fedoraproject.org/message/KSEGD2IWKNUO3DWY4K
QGUQM5BISRWHQE
https://lists.fedoraproject.org/archives/list/package-announce%40
lists.fedoraproject.org/message/KSEGD2IWKNUO3DWY4KQGUQM5BISRWHQE/
https://lists.
fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/messa
ge/LKYHSZQFDNR7RSA7LHVLLIAQMVYCUGBG
https://lists.fedoraproject.org/archives/lis
t/package-announce%40lists.fedoraproject.org/message/LKYHSZQFDNR7RSA7LHVLLIAQMVY
CUGBG/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fe
doraproject.org/message/LNMZJCDHGLJJLXO4OXWJMTVQRNWOC7UL
https://lists.fedorapro
ject.org/archives/list/package-announce%40lists.fedoraproject.org/message/LNMZJC
DHGLJJLXO4OXWJMTVQRNWOC7UL/
https://lists.fedoraproject.org/archives/list/packag
e-announce%40lists.fedoraproject.org/message/VHUHTSXLXGXS7JYKBXTA3VINUPHTNGVU
ht
tps://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproje
ct.org/message/VHUHTSXLXGXS7JYKBXTA3VINUPHTNGVU/
https://lists.fedoraproject.org
/archives/list/package-announce%40lists.fedoraproject.org/message/VSRDIV77HNKUSM
7SJC5BKE5JSHLHU2NK
https://lists.fedoraproject.org/archives/list/package-announc

e%40lists.fedoraproject.org/message/VSRDIV77HNKUSM7SJC5BKE5JSHLHU2NK/
https://li
sts.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/m
essage/WE2I52RHNNU42PX6NZ2RBUHSFFJ2LVZX
https://lists.fedoraproject.org/archives
/list/package-announce%40lists.fedoraproject.org/message/WE2I52RHNNU42PX6NZ2RBUH
SFFJ2LVZX/
https://lists.fedoraproject.org/archives/list/package-announce%40list
s.fedoraproject.org/message/WLPRQ5TWUQQXYWBJM7ECYDAIL2YVKIUH
https://lists.fedor
aproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/WL
PRQ5TWUQQXYWBJM7ECYDAIL2YVKIUH/
https://lists.fedoraproject.org/archives/list/pa
ckage-announce%40lists.fedoraproject.org/message/X6QXN4ORIVF6XBW4WWFE7VNPVC74S45
Y
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedorap
roject.org/message/X6QXN4ORIVF6XBW4WWFE7VNPVC74S45Y/
https://lists.fedoraproject
.org/archives/list/package-announce%40lists.fedoraproject.org/message/XFOIBB4YFI
CHDM7IBOP7PWXW3FX4HLL2
https://lists.fedoraproject.org/archives/list/package-ann
ounce%40lists.fedoraproject.org/message/XFOIBB4YFICHDM7IBOP7PWXW3FX4HLL2/
https:
//lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.o
rg/message/ZB43REMKRQR62NJEI7I5NQ4FSXNLBKRT
https://lists.fedoraproject.org/arch
ives/list/package-announce%40lists.fedoraproject.org/message/ZB43REMKRQR62NJEI7I
5NQ4FSXNLBKRT/
https://lists.fedoraproject.org/archives/list/package-announce%40
lists.fedoraproject.org/message/ZKQSIKIAT5TJ3WSLU3RDBQ35YX4GY4V3
https://lists.f
edoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/messag
e/ZKQSIKIAT5TJ3WSLU3RDBQ35YX4GY4V3/
https://lists.fedoraproject.org/archives/lis
t/package-announce%40lists.fedoraproject.org/message/ZLU6U2R2IC2K64NDPNMV55AUAO6
5MAF4
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fed

Vulnerability Report

oraproject.org/message/ZLU6U2R2IC2K64NDPNMV55AUAO65MAF4/
https://lists.fedorapro
ject.org/archives/list/package-announce@lists.fedoraproject.org/message/2MBEPPC3
6UBVOZZNAXFHKLFGSLCMN5LI
https://lists.fedoraproject.org/archives/list/package-a
nnounce@lists.fedoraproject.org/message/2MBEPPC36UBVOZZNAXFHKLFGSLCMN5LI/
https:
//lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org
/message/3N4NJ7FR4X4FPZUGNTQAPSTVB2HB2Y4A
https://lists.fedoraproject.org/archiv
es/list/package-announce@lists.fedoraproject.org/message/3N4NJ7FR4X4FPZUGNTQAPST
VB2HB2Y4A/
https://lists.fedoraproject.org/archives/list/package-announce@lists.
fedoraproject.org/message/BFQD3KUEMFBHPAPBGLWQC34L4OWL5HAZ
https://lists.fedorap
roject.org/archives/list/package-announce@lists.fedoraproject.org/message/BFQD3K
UEMFBHPAPBGLWQC34L4OWL5HAZ/
https://lists.fedoraproject.org/archives/list/packag
e-announce@lists.fedoraproject.org/message/CLB4TW7KALB3EEQWNWCN7OUIWWVWWCG2
http
s://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.o
rg/message/CLB4TW7KALB3EEQWNWCN7OUIWWVWWCG2/
https://lists.fedoraproject.org/arc
hives/list/package-announce@lists.fedoraproject.org/message/E72T67UPDRXHIDLO3ORO
R25YAMN4GGW5
https://lists.fedoraproject.org/archives/list/package-announce@list
s.fedoraproject.org/message/E72T67UPDRXHIDLO3ORO R25YAMN4GGW5/
https://lists.fedo
raproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FNA
62Q767CFAFHBCDKYNPBMZWB7TWYVU
https://lists.fedoraproject.org/archives/list/pack
age-announce@lists.fedoraproject.org/message/FNA62Q767CFAFHBCDKYNPBMZWB7TWYVU/
h
ttps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraprojec
t.org/message/HT7T2R4MQKLIF4ODV4BDLPARWFPCJ5CZ
https://lists.fedoraproject.org/a
rchives/list/package-announce@lists.fedoraproject.org/message/HT7T2R4MQKLIF4ODV4

Vulnerability Report

BDLPARWFPCJ5CZ/
https://lists.fedoraproject.org/archives/list/package-announce@l
ists.fedoraproject.org/message/JIZSEFC3YKCGABA2BZW6ZJRMDZJMB7PJ
https://lists.fe
doraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/J
IZSEFC3YKCGABA2BZW6ZJRMDZJMB7PJ/
https://lists.fedoraproject.org/archives/list/p
ackage-announce@lists.fedoraproject.org/message/JMEXY22BFG5Q64HQCM5CK2Q7KDKVV4TY
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproj
ect.org/message/JMEXY22BFG5Q64HQCM5CK2Q7KDKVV4TY/
https://lists.fedoraproject.or
g/archives/list/package-announce@lists.fedoraproject.org/message/KSEGD2IWKNUO3DW
Y4KQGUQM5BISRWHQE
https://lists.fedoraproject.org/archives/list/package-announce
@lists.fedoraproject.org/message/KSEGD2IWKNUO3DWY4KQGUQM5BISRWHQE/
https://lists
.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag
e/LKYHSZQFDNR7RSA7LHVLLIAQMVYCUGBG
https://lists.fedoraproject.org/archives/list
/package-announce@lists.fedoraproject.org/message/LKYHSZQFDNR7RSA7LHVLLIAQMVYCUG
BG/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedorap
roject.org/message/LNMZJCDHGLJJLXO4OXWJMTVQRNWOC7UL
https://lists.fedoraproject.
org/archives/list/package-announce@lists.fedoraproject.org/message/LNMZJCDHGLJJL
XO4OXWJMTVQRNWOC7UL/
https://lists.fedoraproject.org/archives/list/package-annou
nce@lists.fedoraproject.org/message/VHUHTSXLXGXS7JYKBXTA3VINUPHTNGVU
https://lis
ts.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/mess
age/VHUHTSXLXGXS7JYKBXTA3VINUPHTNGVU/
https://lists.fedoraproject.org/archives/l
ist/package-announce@lists.fedoraproject.org/message/VSRDIV77HNKUSM7SJC5BKE5JSHL
HU2NK
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedor
aproject.org/message/VSRDIV77HNKUSM7SJC5BKE5JSHLHU2NK/

Vulnerability Report

https://lists.fedoraproje
ct.org/archives/list/package-announce@lists.fedoraproject.org/message/WE2I52RHNN
U42PX6NZ2RBUHSFFJ2LVZX
https://lists.fedoraproject.org/archives/list/package-ann
ounce@lists.fedoraproject.org/message/WE2I52RHNNU42PX6NZ2RBUHSFFJ2LVZX/
https://
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/m
essage/WLPRQ5TWUQQXYWBJM7ECYDAIL2YVKIUH
https://lists.fedoraproject.org/archives
/list/package-announce@lists.fedoraproject.org/message/WLPRQ5TWUQQXYWBJM7ECYDAIL
2YVKIUH/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fe
doraproject.org/message/X6QXN4ORIVF6XBW4WWFE7VNPVC74S45Y
https://lists.fedorapro
ject.org/archives/list/package-announce@lists.fedoraproject.org/message/X6QXN4OR
IVF6XBW4WWFE7VNPVC74S45Y/
https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/XFOIBB4YFICHDM7IBOP7PWXW3FX4HLL2
https:
//lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org
/message/XFOIBB4YFICHDM7IBOP7PWXW3FX4HLL2/
https://lists.fedoraproject.org/archi
ves/list/package-announce@lists.fedoraproject.org/message/ZB43REMKRQR62NJEI7I5NQ
4FSXNLBKRT
https://lists.fedoraproject.org/archives/list/package-announce@lists.
fedoraproject.org/message/ZB43REMKRQR62NJEI7I5NQ4FSXNLBKRT/
https://lists.fedora
project.org/archives/list/package-announce@lists.fedoraproject.org/message/ZKQSI
KIAT5TJ3WSLU3RDBQ35YX4GY4V3
https://lists.fedoraproject.org/archives/list/packag
e-announce@lists.fedoraproject.org/message/ZKQSIKIAT5TJ3WSLU3RDBQ35YX4GY4V3/
htt
ps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.
org/message/ZLU6U2R2IC2K64NDPNMV55AUAO65MAF4
https://lists.fedoraproject.org/arc
hives/list/package-announce@lists.fedoraproject.org/message/ZLU6U2R2IC2K64NDPNMV
55AUAO65MAF4/

https://lists.w3.org/Archives/Public/ietf-http-wg/2023OctDec/0025.
html
https://mailman.nginx.org/pipermail/nginx-devel/2023-October/S36Q5HBXR7CAIM
PLLPRSSSYR4PCMWILK.html
https://martinthomson.github.io/h2-stream-limits/draft-t
homson-httpbis-h2-stream-limits.html
https://msrc.microsoft.com/blog/2023/10/mic
rosoft-response-to-distributed-denial-of-service-ddos-attacks-against-http/2
htt
ps://msrc.microsoft.com/blog/2023/10/microsoft-response-to-distributed-denial-of
-service-ddos-attacks-against-http/2/
https://msrc.microsoft.com/update-guide/vu
lnerability/CVE-2023-44487
https://my.f5.com/manage/s/article/K000137106
https:/
/netty.io/news/2023/10/10/4-1-100-Final.html
https://news.ycombinator.com/item?i
d=37830987
https://news.ycombinator.com/item?id=37830998
https://news.ycombinato
r.com/item?id=37831062
https://news.ycombinator.com/item?id=37837043
https://nod
ejs.org/en/blog/vulnerability/october-2023-security-releases
https://nvd.nist.go
v/vuln/detail/CVE-2023-44487
https://openssf.org/blog/2023/10/10/http-2-rapid-re
set-vulnerability-highlights-need-for-rapid-response
https://openssf.org/blog/20
23/10/10/http-2-rapid-reset-vulnerability-highlights-need-for-rapid-response/
ht
tps://pkg.go.dev/vuln/GO-2023-2102
https://seanmonstar.com/post/7307941511369359
36/hyper-http2-rapid-reset-unaffected
https://security.gentoo.org/glsa/202311-09
https://security.netapp.com/advisory/ntap-20231016-0001

Vulnerability Report

https://security.netapp
.com/advisory/ntap-20231016-0001/
https://security.netapp.com/advisory/ntap-2024
0426-0007
https://security.netapp.com/advisory/ntap-20240426-0007/
https://secur
ity.netapp.com/advisory/ntap-20240621-0006
https://security.netapp.com/advisory/
ntap-20240621-0006/
https://security.netapp.com/advisory/ntap-20240621-0007
http
s://security.netapp.com/advisory/ntap-20240621-0007/
https://security.paloaltone
tworks.com/CVE-2023-44487
https://tomcat.apache.org/security-10.html#Fixed_in_Ap
ache_Tomcat_10.1.14
https://tomcat.apache.org/security-11.html#Fixed_in_Apache_T
omcat_11.0.0-M12
https://tomcat.apache.org/security-8.html
https://tomcat.apache
.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.94
https://tomcat.apache.org/sec
urity-9.html#Fixed_in_Apache_Tomcat_9.0.81
https://ubuntu.com/security/CVE-2023-
44487
https://ubuntu.com/security/notices/USN-6427-1
https://ubuntu.com/security
/notices/USN-6427-2
https://ubuntu.com/security/notices/USN-6438-1
https://ubunt
u.com/security/notices/USN-6505-1
https://ubuntu.com/security/notices/USN-6574-1
https://ubuntu.com/security/notices/USN-6754-1
https://ubuntu.com/security/noti
ces/USN-6994-1
https://ubuntu.com/security/notices/USN-7067-1

Vulnerability Report

https://ubuntu.com
/security/notices/USN-7410-1
https://ubuntu.com/security/notices/USN-7469-1
http
s://ubuntu.com/security/notices/USN-7469-2
https://ubuntu.com/security/notices/U
SN-7469-3
https://ubuntu.com/security/notices/USN-7469-4
https://www.bleepingcom
puter.com/news/security/new-http-2-rapid-reset-zero-day-attack-breaks-ddos-recor
ds
https://www.bleepingcomputer.com/news/security/new-http-2-rapid-reset-zero-da
y-attack-breaks-ddos-records/
https://www.cisa.gov/known-exploited-vulnerabiliti
es-catalog
https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-
vulnerability-cve-2023-44487
https://www.cve.org/CVERecord?id=CVE-2023-44487
htt
ps://www.darkreading.com/cloud/internet-wide-zero-day-bug-fuels-largest-ever-ddo
s-event
https://www.debian.org/security/2023/dsa-5521
https://www.debian.org/sec
urity/2023/dsa-5522
https://www.debian.org/security/2023/dsa-5540
https://www.de
bian.org/security/2023/dsa-5549
https://www.debian.org/security/2023/dsa-5558
ht
tps://www.debian.org/security/2023/dsa-5570
https://www.eclipse.org/lists/jetty-
announce/msg00181.html
https://www.haproxy.com/blog/haproxy-is-not-affected-by-t
he-http-2-rapid-reset-attack-cve-2023-44487
https://www.mail-archive.com/haproxy
@formilux.org/msg44134.html
https://www.netlify.com/blog/netlify-successfully-mi

Vulnerability Report

tigates-cve-2023-44487
https://www.netlify.com/blog/netlify-successfully-mitigat
es-cve-2023-44487/
https://www.nginx.com/blog/http-2-rapid-reset-attack-impactin
g-f5-nginx-products
https://www.nginx.com/blog/http-2-rapid-reset-attack-impacti
ng-f5-nginx-products/
https://www.openwall.com/lists/oss-security/2023/10/10/6
h
ttps://www.phoronix.com/news/HTTP2-Rapid-Reset-Attack
https://www.theregister.co
m/2023/10/10/http2_rapid_reset_zeroday
https://www.theregister.com/2023/10/10/ht
tp2_rapid_reset_zeroday/
https://www.vicarius.io/vsociety/posts/rapid-reset-cve-
2023-44487-dos-in-http2-understanding-the-root-cause

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-45648
Title:	tomcat: incorrectly parsed http trailer headers can cause request smuggling
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.0-M12, 10.1.14, 9.0.81, 8.5.94
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	CWE-20
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-45648
Description:	Improper Input Validation vulnerability in Apache Tomcat.TomcatÂ from 11.0.0-M1 t hrough 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A sp ecially crafted, invalid trailer header could cause Tomcat to treat a single r equest as multiple requests leading to the possibility of request smuggling whe n behind a reverse proxy. Users are recommended to upgrade to version 11.0.0-M1 2 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issu e.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2023/10/10/10 https://access.redhat.c om/errata/RHSA-2024:0474 https://access.redhat.com/security/cve/CVE-2023-45648 h ttps://bugzilla.redhat.com/2235370 https://bugzilla.redhat.com/2243749 https://b ugzilla.redhat.com/2243751 https://bugzilla.redhat.com/2243752 https://errata.al

Vulnerability Report

malinux.org/9/ALSA-2024-0474.html
https://github.com/apache/tomcat
https://githu
b.com/apache/tomcat/commit/59583245639d8c42ae0009f4a4a70464d3ea70a0
https://gith
ub.com/apache/tomcat/commit/8ecff306507be8e4fd3adee1ae5de1ea6661a8f4
https://git
hub.com/apache/tomcat/commit/c83fe47725f7ae9ae213568d9039171124fb7ec6
https://gi
thub.com/apache/tomcat/commit/eb5c094e5560764cda436362254997511a3ca1f6
https://l
inux.oracle.com/cve/CVE-2023-45648.html
https://linux.oracle.com/errata/ELSA-202
4-0474.html
https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp
htt
ps://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
https://nvd.nist
.gov/vuln/detail/CVE-2023-45648
https://security.netapp.com/advisory/ntap-202311
03-0007
https://security.netapp.com/advisory/ntap-20231103-0007/
https://ubuntu.
com/security/notices/USN-7106-1
https://www.cve.org/CVERecord?id=CVE-2023-45648
https://www.debian.org/security/2023/dsa-5521
https://www.debian.org/security/20
23/dsa-5522
https://www.openwall.com/lists/oss-security/2023/10/10/10

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-24549
Title:	Tomcat: HTTP/2 header handling DoS
Package:	org.apache.tomcat.embed:tomcat-embed-core
Package ID:	org.apache.tomcat.embed:tomcat-embed-core:9.0.56
Installed Version:	9.0.56
Fixed Version:	8.5.99, 9.0.86, 10.1.19, 11.0.0-M17
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	7.5
CWE:	CWE-20
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-24549
Description:	Denial of Service due to improper input validation vulnerability for HTTP/2 requ ests in Apache Tomcat. When processing an HTTP/2 request, if the request exceede d any of the configured limits for headers, the associated HTTP/2 stream was not reset until after all of the headers had been processed.This issue affects Apac he Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, fr om 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98. Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2024/03/13/3 https://access.redhat.co m/errata/RHSA-2024:3307 https://access.redhat.com/security/cve/CVE-2024-24549 ht tps://bugzilla.redhat.com/2269607 https://bugzilla.redhat.com/2269608 https://bu gzilla.redhat.com/show_bug.cgi?id=2269607 https://bugzilla.redhat.com/show_bug.c gi?id=2269608 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23672 http s://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24549 https://errata.almalin

Vulnerability Report

ux.org/9/ALSA-2024-3307.html
https://errata.rockylinux.org/RLSA-2024:3307
https:
//github.com/apache/tomcat
https://github.com/apache/tomcat/commit/0cac540a88222
0231ba7a82330483cbd5f6b1f96
https://github.com/apache/tomcat/commit/810f49d5ff6d
64b704af85d5b8d0aab9ec3c83f5
https://github.com/apache/tomcat/commit/8e03be9f269
8f2da9027d40b9e9c0c9429b74dc0
https://github.com/apache/tomcat/commit/d07c82194e
db69d99b438828fe2cbfadbb207843
https://linux.oracle.com/cve/CVE-2024-24549.html
https://linux.oracle.com/errata/ELSA-2024-3666.html
https://lists.apache.org/thr
ead/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg
https://lists.debian.org/debian-lts-announc
e/2024/04/msg00001.html
https://lists.fedoraproject.org/archives/list/package-an
nounce@lists.fedoraproject.org/message/3UWIS5MMGYDZBLJYT674ZI5AWFHDZ46B
https://
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/m
essage/3UWIS5MMGYDZBLJYT674ZI5AWFHDZ46B/
https://lists.fedoraproject.org/archive
s/list/package-announce@lists.fedoraproject.org/message/736G4GPZWS2DSQO5WKXO3G6O
MZKFEK55
https://lists.fedoraproject.org/archives/list/package-announce@lists.fe
doraproject.org/message/736G4GPZWS2DSQO5WKXO3G6OMZKFEK55/
https://nvd.nist.gov/v
uln/detail/CVE-2024-24549
https://security.netapp.com/advisory/ntap-20240402-000
2
https://security.netapp.com/advisory/ntap-20240402-0002/
https://www.cve.org/C
VERecord?id=CVE-2024-24549

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-23672
Title:	Tomcat: WebSocket DoS with incomplete closing handshake
Package:	org.apache.tomcat.embed:tomcat-embed-websocket
Package ID:	org.apache.tomcat.embed:tomcat-embed-websocket:9.0.56
Installed Version:	9.0.56
Fixed Version:	11.0.0-M17, 10.1.19, 9.0.86, 8.5.99
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.3
CWE:	CWE-459
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-23672
Description:	Denial of Service via incomplete cleanup vulnerability in Apache Tomcat. It was possible for WebSocket clients to keep WebSocket connections open leading to increased resource consumption.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98. Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2024/03/13/4 https://access.redhat.co m/errata/RHSA-2024:3307 https://access.redhat.com/security/cve/CVE-2024-23672 ht tps://bugzilla.redhat.com/2269607 https://bugzilla.redhat.com/2269608 https://bu gzilla.redhat.com/show_bug.cgi?id=2269607 https://bugzilla.redhat.com/show_bug.c gi?id=2269608 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23672 http s://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24549 https://errata.almalin ux.org/9/ALSA-2024-3307.html

Vulnerability Report

https://errata.rockylinux.org/RLSA-2024:3307
https:
//github.com/apache/tomcat
https://github.com/apache/tomcat/commit/0052b374684b6
13b0c849899b325ebe334ac6501
https://github.com/apache/tomcat/commit/0052b374684b
613b0c849899b325ebe334ac6501 (10.1.19)
https://github.com/apache/tomcat/commit/3
631adb1342d8bbd8598802a12b63ad02c37d591
https://github.com/apache/tomcat/commit/
52d6650e062d880704898d7d8c1b2b7a3efe8068
https://github.com/apache/tomcat/commit
/52d6650e062d880704898d7d8c1b2b7a3efe8068 (9.0.86)
https://github.com/apache/tom
cat/commit/b0e3b1bd78de270d53e319d7cb79eb282aa53cb9
https://linux.oracle.com/cve
/CVE-2024-23672.html
https://linux.oracle.com/errata/ELSA-2024-3666.html
https:/
/lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f
https://lists.debian.o
rg/debian-lts-announce/2024/04/msg00001.html
https://lists.fedoraproject.org/arc
hives/list/package-announce@lists.fedoraproject.org/message/3UWIS5MMGYDZBLJYT674
ZI5AWFHDZ46B
https://lists.fedoraproject.org/archives/list/package-announce@list
s.fedoraproject.org/message/3UWIS5MMGYDZBLJYT674ZI5AWFHDZ46B/
https://lists.fedo
raproject.org/archives/list/package-announce@lists.fedoraproject.org/message/736
G4GPZWS2DSQO5WKXO3G6OMZKFEK55
https://lists.fedoraproject.org/archives/list/pack
age-announce@lists.fedoraproject.org/message/736G4GPZWS2DSQO5WKXO3G6OMZKFEK55/
h
ttps://nvd.nist.gov/vuln/detail/CVE-2024-23672
https://security.netapp.com/advis
ory/ntap-20240402-0002
https://security.netapp.com/advisory/ntap-20240402-0002/

Vulnerability Report

https://ubuntu.com/security/notices/USN-7106-1
https://www.cve.org/CVERecord?id=
CVE-2024-23672

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2020-13959
Title:	velocity: XSS in the default error page for VelocityView
Package:	org.apache.velocity:velocity-tools
Package ID:	org.apache.velocity:velocity-tools:2.0
Installed Version:	2.0
Fixed Version:	N/A
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.1
CWE:	CWE-79
Primary URL:	https://avd.aquasec.com/nvd/cve-2020-13959
Description:	The default error page for VelocityView in Apache Velocity Tools prior to 3.1 reflects back the vm file that was entered as part of the URL. An attacker can set an XSS payload file as this vm file in the URL which results in this payload being executed. XSS vulnerabilities allow attackers to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.

Vulnerability Report

References:	http://www.openwall.com/lists/oss-security/2021/03/10/2 https://access.redhat.co m/security/cve/CVE-2020-13959 https://lists.apache.org/thread.html/r6802a38c3041 059e763a1aadd7b37fe95de75408144b5805e29b84e3%40%3Cuser.velocity.apache.org%3E ht tps://lists.apache.org/thread.html/r6802a38c3041059e763a1aadd7b37fe95de75408144b 5805e29b84e3@%3Cuser.velocity.apache.org%3E https://lists.apache.org/thread.html /r97edad0655770342d2d36620fb1de50b142fcd6c4f5c53dd72ca41d7%40%3Cuser.velocity.ap ache.org%3E https://lists.apache.org/thread.html/r97edad0655770342d2d36620fb1de5 0b142fcd6c4f5c53dd72ca41d7@%3Cuser.velocity.apache.org%3E https://lists.apache.o rg/thread.html/rb042f3b0090e419cc9f5a3d32cf0baff283ccd6fcb1caea61915d6b6%40%3Cco mmits.velocity.apache.org%3E https://lists.apache.org/thread.html/rb042f3b0090e4

Vulnerability Report

19cc9f5a3d32cf0baff283ccd6fcb1caea61915d6b6@%3Ccommits.velocity.apache.org%3E
ht
tps://lists.apache.org/thread.html/rf9868c564cff7adfd5283563f2309b93b3e496354a21
1a57503b2f72%40%3Cannounce.apache.org%3E
https://lists.apache.org/thread.html/rf
9868c564cff7adfd5283563f2309b93b3e496354a211a57503b2f72@%3Cannounce.apache.org%3
E
https://lists.debian.org/debian-lts-announce/2021/03/msg00021.html
https://nvd
.nist.gov/vuln/detail/CVE-2020-13959
https://security.gentoo.org/glsa/202107-52
https://ubuntu.com/security/notices/USN-6282-1
https://www.cve.org/CVERecord?id=
CVE-2020-13959
https://www.openwall.com/lists/oss-security/2021/03/10/2

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-36033
Title:	jsoup: The jsoup cleaner may incorrectly sanitize crafted XSS attempts if SafeLi st.preserveRelativeLinks is enabled
Package:	org.jsoup:jsoup
Package ID:	org.jsoup:jsoup:1.10.2
Installed Version:	1.10.2
Fixed Version:	1.15.3
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.1
CWE:	CWE-79, CWE-87
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-36033
Description:	jsoup is a Java HTML parser, built for HTML editing, cleaning, scraping, and cro ss-site scripting (XSS) safety. jsoup may incorrectly sanitize HTML including `j avascript:` URL expressions, which could allow XSS attacks when a reader subsequ ently clicks that link. If the non-default `SafeList.preserveRelativeLinks` opti on is enabled, HTML including `javascript:` URLs that have been crafted with con trol characters will not be sanitized. If the site that this HTML is published o n does not set a Content Security Policy, an XSS attack is then possible. This i ssue is patched in jsoup 1.15.3. Users should upgrade to this version. Additiona lly, as the unsanitized input may have been persisted, old content should be cle aned again using the updated version. To remediate this issue without immediatel y upgrading: - disable `SafeList.preserveRelativeLinks`, which will rewrite inpu t URLs as absolute URLs - ensure an appropriate [Content Security Policy](https: //developer.mozilla.org/en-US/docs/Web/HTTP/CSP) is defined. (This should be use d regardless of upgrading, as a defence-in-depth best practice.)

Vulnerability Report

References:

https://access.redhat.com/security/cve/CVE-2022-36033

https://github.com/jhy/jso

up

https://github.com/jhy/jsoup/releases/tag/jsoup-1.15.3

https://github.com/jhy

/jsoup/security/advisories/GHSA-gp7f-rwcx-9369

https://jsoup.org/news/release-1.

15.3

https://nvd.nist.gov/vuln/detail/CVE-2022-36033

Vulnerability Report

https://security.netapp.com
/advisory/ntap-20221104-0006
https://security.netapp.com/advisory/ntap-20221104-
0006/
https://www.cve.org/CVERecord?id=CVE-2022-36033

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-34055
Title:	spring-boot: org.springframework.boot: spring-boot-actuator class vulnerable to denial of service
Package:	org.springframework.boot:spring-boot-actuator
Package ID:	org.springframework.boot:spring-boot-actuator:2.6.2
Installed Version:	2.6.2
Fixed Version:	2.7.18, 3.0.13, 3.1.6
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	N/A
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-34055
Description:	In Spring Boot versions 2.7.0 - 2.7.17, 3.0.0-3.0.12 and 3.1.0-3.1.5, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC or Spring WebFlux * org.springframework.boot:spring-boot-actuatorÂ is on the classpath

Vulnerability Report

References:

https://access.redhat.com/security/cve/CVE-2023-34055

https://github.com/spring-

projects/spring-boot

https://github.com/spring-projects/spring-boot/commit/5490e

73922b37a7f0bdde43eb318cb1038b45d60

https://nvd.nist.gov/vuln/detail/CVE-2023-34

055

https://security.netapp.com/advisory/ntap-20231221-0010

https://security.net

app.com/advisory/ntap-20231221-0010/

https://security.snyk.io/vuln/SNYK-JAVA-ORG

SPRINGFRAMEWORKBOOT-6226862

https://spring.io/security/cve-2023-34055

Vulnerability Report

https://ww
w.cve.org/CVERecord?id=CVE-2023-34055

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-38820
Title:	The fix for CVE-2022-22968 made disallowedFieldspatterns in DataBinder ...
Package:	org.springframework:spring-context
Package ID:	org.springframework:spring-context:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.1.14
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	CWE-178
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-38820
Description:	The fix for CVE-2022-22968 made disallowedFieldsÂ patterns in DataBinderÂ case ins ensitive. However, String.toLowerCase()Â has some Locale dependent exceptions tha t could potentially result in fields not protected as expected.
References:	https://github.com/spring-projects/spring-framework https://github.com/spring-pr ojects/spring-framework/commit/23656aebc6c7d0f9faff1080981eb4d55eff296c https:// github.com/spring-projects/spring-framework/commits/v6.2.0-RC2 https://nvd.nist. gov/vuln/detail/CVE-2024-38820 https://security.netapp.com/advisory/ntap-2024112 9-0003 https://security.netapp.com/advisory/ntap-20241129-0003/ https://spring.i o/security/cve-2024-38820

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-22950
Title:	spring-expression: Denial of service via specially crafted SpEL expression
Package:	org.springframework:spring-expression
Package ID:	org.springframework:spring-expression:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.3.17, 5.2.20.RELEASE
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.5
CWE:	CWE-770
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-22950
Description:	n Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cau se a denial of service condition.
References:	https://access.redhat.com/security/cve/CVE-2022-22950 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/commit/83ac65915871067c39a4fb255e0d484c785c0c11 https://github.com/spring-projects/spring-framework/issues/28145 https://github.com/spring-projects/spring-framework/issues/28257 https://github.com/spring-projects/spring-framework/releases/tag/v5.2.20.RELEASE https://github.com/spring-projects/spring-framework/releases/tag/v5.3.17 https://nvd.nist.gov/vuln/detail/CVE-2022-22950 https://tanzu.vmware.com/security/cve-2022-22950 https://www.cve.org/CVERecord?id=CVE-2022-22950

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2023-20861
Title:	springframework: Spring Expression DoS Vulnerability
Package:	org.springframework:spring-expression
Package ID:	org.springframework:spring-expression:5.3.14
Installed Version:	5.3.14
Fixed Version:	6.0.7, 5.3.26, 5.2.23.RELEASE
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.5
CWE:	CWE-400
Primary URL:	https://avd.aquasec.com/nvd/cve-2023-20861
Description:	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2. 22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) co ndition.
References:	https://access.redhat.com/security/cve/CVE-2023-20861 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/commit/430fc25acad2e85cbdddcd52b64481691f03ebd1 https://github.com/spring-projects/spring-framework/commit/52c93b1c4b24d70de233a958e60e7c5822bd274f https://github.com/spring-projects/spring-framework/commit/935c29e3ddba5b19951e54f6685c70ed45d9cbe5 https://nvd.nist.gov/vuln/detail/CVE-2023-20861 https://security.netapp.com/advisory/ntap-20230420-0007 https://security.netapp.com/advisory/ntap-20230420-0007/ https://spring.io/blog/2023/03/20/spring-framework-6-0-7-and-5-3-26-fix-cve-2023-20860-and-cve-2023-20861 https://spring.io/security/cve-2023-20861 https://www.cve.org/CVERecord?id=CVE-2023-20861

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-38808
Title:	spring-expression: Denial of service when processing a specially crafted Spring Expression Language expression
Package:	org.springframework:spring-expression
Package ID:	org.springframework:spring-expression:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.3.39
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	4.3
CWE:	CWE-770
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-38808
Description:	In Spring Framework versions 5.3.0 - 5.3.38 and older unsupported versions, it is possible for a user to provide a specially crafted Spring Expression Language (SpEL) expression that may cause a denial of service (DoS) condition. Specifically, an application is vulnerable when the following is true: * The application evaluates user-supplied SpEL expressions.
References:	https://access.redhat.com/security/cve/CVE-2024-38808 https://github.com/spring-projects/spring-framework https://github.com/spring-projects/spring-framework/commit/26f2dad388499faecf99e75b8856788e95d8d658 https://github.com/spring-projects/spring-framework/commit/f44d13cb7816e586b86c02421af4f5498391111c https://nvd.nist.gov/vuln/detail/CVE-2024-38808 https://security.netapp.com/advisory/ntap-20240920-0002/ https://spring.io/security/cve-2024-38808 https://www.cve.org/CVERecord?id=CVE-2024-38808

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-38809
Title:	org.springframework:spring-web: Spring Framework DoS via conditional HTTP reques t
Package:	org.springframework:spring-web
Package ID:	org.springframework:spring-web:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.3.38, 6.0.23, 6.1.12
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	CWE-400
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-38809
Description:	Applications that parse ETags from "If-Match" or "If-None-Match" request headers are vulnerable to DoS attack. Users of affected versions should upgrade to the corresponding fixed version. Users of older, unsupported versions could enforc e a size limit on "If-Match" and "If-None-Match" headers, e.g. through a Filter.

Vulnerability Report

References:

http://github.com/spring-projects/spring-framework

https://access.redhat.com/sec

urity/cve/CVE-2024-38809

https://github.com/spring-projects/spring-framework

htt

ps://github.com/spring-projects/spring-framework/commit/582bfccbb72e5c8959a0b472

d1dc7d03a20520f3

https://github.com/spring-projects/spring-framework/commit/8d16

a50907c11f7e6b407d878a26e84eba08a533

https://github.com/spring-projects/spring-f

ramework/commit/bb17ad8314b81850a939fd265fb53b3361705e85

https://github.com/spri

ng-projects/spring-framework/issues/33372

https://nvd.nist.gov/vuln/detail/CVE-2

024-38809

Vulnerability Report

https://security.netapp.com/advisory/ntap-20240920-0003/
https://sprin
g.io/security/cve-2024-38809
https://www.cve.org/CVERecord?id=CVE-2024-38809

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-38828
Title:	org.springframework:spring-webmvc: DoS via Spring MVC controller method with byte[] parameter
Package:	org.springframework:spring-webmvc
Package ID:	org.springframework:spring-webmvc:5.3.14
Installed Version:	5.3.14
Fixed Version:	5.3.42
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.3
CWE:	CWE-400
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-38828
Description:	Spring MVC controller methods with an @RequestBody byte[]Â method parameter are vulnerable to a DoS attack.
References:	https://access.redhat.com/security/cve/CVE-2024-38828 https://github.com/spring-projects/spring-framework https://nvd.nist.gov/vuln/detail/CVE-2024-38828 https://security.netapp.com/advisory/ntap-20250509-0009 https://security.netapp.com/advisory/ntap-20250509-0009/ https://spring.io/security/cve-2024-38828 https://www.cve.org/CVERecord?id=CVE-2024-38828

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-38749
Title:	snakeyaml: Uncaught exception in org.yaml.snakeyaml.composer.Composer.composeSeq uenceNode
Package:	org.yaml:snakeyaml
Package ID:	org.yaml:snakeyaml:1.29
Installed Version:	1.29
Fixed Version:	1.31
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.5
CWE:	CWE-121, CWE-787
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-38749
Description:	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Ser vice attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.
References:	https://access.redhat.com/security/cve/CVE-2022-38749 https://arxiv.org/pdf/2306 .05534.pdf https://bitbucket.org/snakeyaml/snakeyaml https://bitbucket.org/snake yaml/snakeyaml/issues/525/got-stackoverflowerror-for-many-open https://bugs.chro mium.org/p/oss-fuzz/issues/detail?id=47024 https://lists.debian.org/debian-lts-a nnounce/2022/10/msg00001.html https://nvd.nist.gov/vuln/detail/CVE-2022-38749 ht tps://security.gentoo.org/glsa/202305-28 https://security.netapp.com/advisory/nt ap-20240315-0010 https://security.netapp.com/advisory/ntap-20240315-0010/ https: //ubuntu.com/security/notices/USN-5944-1 https://www.cve.org/CVERecord?id=CVE-20 22-38749

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-38750
Title:	snakeyaml: Uncaught exception in org.yaml.snakeyaml.constructor.BaseConstructor.constructObject
Package:	org.yaml:snakeyaml
Package ID:	org.yaml:snakeyaml:1.29
Installed Version:	1.29
Fixed Version:	1.31
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	5.5
CWE:	CWE-121, CWE-787
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-38750
Description:	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.
References:	https://access.redhat.com/security/cve/CVE-2022-38750 https://bitbucket.org/snakeyaml/snakeyaml https://bitbucket.org/snakeyaml/snakeyaml/issues/526/stackoverflow-oss-fuzz-47027 https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47027 https://lists.debian.org/debian-lts-announce/2022/10/msg00001.html https://nvd.nist.gov/vuln/detail/CVE-2022-38750 https://security.gentoo.org/glsa/202305-28 https://security.netapp.com/advisory/ntap-20240315-0010 https://security.netapp.com/advisory/ntap-20240315-0010/ https://ubuntu.com/security/notices/USN-5944-1 https://www.cve.org/CVERecord?id=CVE-2022-38750

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-38751
Title:	snakeyaml: Uncaught exception in java.base/java.util.regex.Pattern$Ques.match
Package:	org.yaml:snakeyaml
Package ID:	org.yaml:snakeyaml:1.29
Installed Version:	1.29
Fixed Version:	1.31
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.5
CWE:	CWE-121, CWE-787
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-38751
Description:	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.
References:	https://access.redhat.com/security/cve/CVE-2022-38751 https://bitbucket.org/snakeyaml/snakeyaml https://bitbucket.org/snakeyaml/snakeyaml/issues/530/stackoverflow-oss-fuzz-47039 https://bitbucket.org/snakeyaml/snakeyaml/src/master/src/test/java/org/yaml/snakeyaml/issues/issue530/Fuzzy47039Test.java https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47039 https://lists.debian.org/debian-lts-announce/2022/10/msg00001.html https://nvd.nist.gov/vuln/detail/CVE-2022-38751 https://security.gentoo.org/glsa/202305-28 https://security.netapp.com/advisory/ntap-20240315-0010 https://security.netapp.com/advisory/ntap-20240315-0010/ https://ubuntu.com/security/notices/USN-5944-1 https://www.cve.org/CVERecord?id=CVE-2022-38751

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-38752
Title:	snakeyaml: Uncaught exception in java.base/java.util.ArrayList.hashCode
Package:	org.yaml:snakeyaml
Package ID:	org.yaml:snakeyaml:1.29
Installed Version:	1.29
Fixed Version:	1.32
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.5
CWE:	CWE-121, CWE-787
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-38752
Description:	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Ser vice attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack-overflow.
References:	https://access.redhat.com/security/cve/CVE-2022-38752 https://bitbucket.org/snak eyaml/snakeyaml https://bitbucket.org/snakeyaml/snakeyaml/issues/531/stackoverfl ow-oss-fuzz-47081 https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47081 ht tps://nvd.nist.gov/vuln/detail/CVE-2022-38752 https://security.gentoo.org/glsa/2 02305-28 https://security.netapp.com/advisory/ntap-20240315-0009 https://securit y.netapp.com/advisory/ntap-20240315-0009/ https://www.cve.org/CVERecord?id=CVE-2 022-38752

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2022-41854
Title:	dev-java/snakeyaml: DoS via stack overflow
Package:	org.yaml:snakeyaml
Package ID:	org.yaml:snakeyaml:1.29
Installed Version:	1.29
Fixed Version:	1.32
Source:	ghsa
Severity:	MEDIUM
CVSS Score:	6.5
CWE:	CWE-121, CWE-787
Primary URL:	https://avd.aquasec.com/nvd/cve-2022-41854
Description:	Those using Snakeyaml to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an at tacker may supply content that causes the parser to crash by stack overflow. Thi s effect may support a denial of service attack.

Vulnerability Report

References:	https://access.redhat.com/security/cve/CVE-2022-41854 https://bitbucket.org/snak eyaml/snakeyaml https://bitbucket.org/snakeyaml/snakeyaml/commits/e230a1758842be ec93d28eddfde568c21774780a https://bitbucket.org/snakeyaml/snakeyaml/issues/531 https://bitbucket.org/snakeyaml/snakeyaml/issues/543/stackoverflow-oss-fuzz-5035 5 https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50355 https://lists.fedo raproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3 DDXEXXWAZGF5AVHIPGFPXIWL6TSMKJE https://lists.fedoraproject.org/archives/list/pa ckage-announce%40lists.fedoraproject.org/message/3DDXEXXWAZGF5AVHIPGFPXIWL6TSMKJ E/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedora project.org/message/7MKE4XWRXTH32757H7QJU4ACS67DYDCR https://lists.fedoraproject .org/archives/list/package-announce%40lists.fedoraproject.org/message/7MKE4XWRXT

Vulnerability Report

H32757H7QJU4ACS67DYDCR/
https://lists.fedoraproject.org/archives/list/package-an
nounce%40lists.fedoraproject.org/message/KSPAJ5Y45A4ZDION2KN5RDWLHK4XKY2J
https:
//lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.o
rg/message/KSPAJ5Y45A4ZDION2KN5RDWLHK4XKY2J/
https://lists.fedoraproject.org/arc
hives/list/package-announce@lists.fedoraproject.org/message/3DDXEXXWAZGF5AVHIPGF
PXIWL6TSMKJE
https://lists.fedoraproject.org/archives/list/package-announce@list
s.fedoraproject.org/message/7MKE4XWRXTH32757H7QJU4ACS67DYDCR
https://lists.fedor
aproject.org/archives/list/package-announce@lists.fedoraproject.org/message/KSPA
J5Y45A4ZDION2KN5RDWLHK4XKY2J
https://nvd.nist.gov/vuln/detail/CVE-2022-41854
htt
ps://security.netapp.com/advisory/ntap-20240315-0009
https://security.netapp.com
/advisory/ntap-20240315-0009/
https://security.netapp.com/advisory/ntap-20240621
-0006
https://security.netapp.com/advisory/ntap-20240621-0006/
https://www.cve.o
rg/CVERecord?id=CVE-2022-41854

Vulnerability Report

Artifact Name:	.
Target:	pom.xml
Vulnerability ID:	CVE-2024-12801
Title:	logback-core: SaxEventRecorder vulnerable to Server-Side Request Forgery (SSRF) attacks
Package:	ch.qos.logback:logback-core
Package ID:	ch.qos.logback:logback-core:1.2.9
Installed Version:	1.2.9
Fixed Version:	1.5.13, 1.3.15
Source:	ghsa
Severity:	LOW
CVSS Score:	N/A
CWE:	CWE-918
Primary URL:	https://avd.aquasec.com/nvd/cve-2024-12801
Description:	Server-Side Request Forgery (SSRF) in SaxEventRecorder by QOS.CH logback version 0.1 to 1.3.14 and 1.4.0 to 1.5.12Â on the Java platform, allows an attacker to forge requests by compromising logback configuration files in XML. The attac ks involves the modification of DOCTYPE declaration inÂ XML configuration files.
References:	https://access.redhat.com/security/cve/CVE-2024-12801 https://github.com/qos-ch/ logback https://github.com/qos-ch/logback/commit/5f05041cba4c4ac0a62748c5c527a2d a48999f2d https://logback.qos.ch/news.html#1.3.15 https://logback.qos.ch/news.ht ml#1.5.13 https://nvd.nist.gov/vuln/detail/CVE-2024-12801 https://www.cve.org/CV ERecord?id=CVE-2024-12801