jayaram krishna kumar Follow
Jun 5, 2020 · 3 min read · Listen

WhiteSource Log injection Vulnerability-CVE -2020-5304

Log Injection Vulnerability Description:

Applications typically use log files to store a history of events or transactions for later review, statistics gathering or debugging. Depending on the nature of the application, the task of reviewing log files may be performed manually on an as-needed basis or automated with a tool that automatically culls logs for important events or trending information.

Writing invalidated user input to log files can allow an attacker to forge log entries or inject malicious content into the logs. This is called log injection.

Log injection vulnerabilities occur when:

1. Data enters an application from an untrusted source.

2. The data is written to an application or system log file.

Successful log injection attacks can cause:

1. Injection of new/bogus log events (log forging via log injection)

2. Injection of XSS attacks, hoping that the malicious log event is viewed in a vulnerable web application

3. Injection of commands that parsers (like PHP parsers) could execute

Log Forging:

In the most benign case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters. If the log file is processed automatically, the attacker can render the file unusable by corrupting the format of the file or injecting unexpected characters. A more subtle attack might involve skewing the log file statistics. Forged or otherwise, corrupted log files can be used to cover an attacker's tracks or even to implicate another party in the commission of a malicious act.

Small Description On WhiteSource Software Composition Analysis Tool:

WhiteSource — Manage Your Open Source Security and Compliance Risks. WhiteSource is the leading solution for agile open source security and license compliance management. It integrates with your development environments and DevOps pipeline to detect open source libraries with security or compliance issues in real-time. WhiteSource doesn't only alert on issues, it also provides actionable, validated remediation paths to enable quick resolution and automated policy enforcement to speed up time-to-fix. It also helps you focus on what matters by prioritizing remediation based on whether your code is actually using a vulnerable method or not and guaranteeing zero false positives. It got you covered with support for over 200 programming languages, and continuous tracking of multiple open source vulnerabilities databases including the NVD, security advisories, peer-reviewed vulnerability knowledge bases, and open source projects issue trackers.

Authentication Needed To Exploit It?

No authentication needed.

Vulnerability Story Details:

We use WhiteSource for software composition analysis for the majority of our application. During my daily routine, I was trying to login to our WhiteSource dashboard and observed a crazy thing happening while it was trying to authenticate using SAML exchange, which is like in the below URL.

GET https://whitesource-dashboard-url.com/saml/login?idp=http://IDP-ENDPOINT-URL/METADATA

I know each and every request we hit to https:// whitesource-dashboard-url.com will store a log entry in $path/Wildfly-xx-final/standalone/log/server.log(WhiteSource web application server works using Jboss(Wildfly) server) so I quickly login to WhiteSource application server and check the recent log and found that the same URL in the log.

Since "idp" parameter is taking the user input I quickly changed it to https://whitesource-dashboard-url.com/saml/login?idp=http://internalURL to check for SSRF condition and no LUCK on it, why because IDP server meta is already fed in Whitesource server so before making a URL call its cross-validating the IDP server URL which it already has. But still, with curiosity, I want to check the server logs at the WhiteSource app server and I found few warnings and errors related to SAML stuff with the internal URL I provided as input to the IDP parameter.

What if I give some special character as input and see the logs, and after few tries, I came up with the below URL where I was able to successfully injected new line and carriage return character and are reflecting in logs.

https:// whitesource-dashboard-url.com/saml/login?idp=<vulnerable URL with CRLF encoded characters %0A%0D>

More info on encoded values:

https://www.eso.org/~ndelmott/url_encode.html

Video PoC:

https://youtu.be/U0sQayhfNqM

Reported: 4nd Jan 2020

Fixed:4th June 2020

Effect version: All version < 20.4.1

Log Injection Whitesource Jayaram Yalla Log Forging