



CVE-2020-5304

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-5304
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-08 17:15:00 UTC
Updated	2023-11-07 03:23:00 UTC
Description	The dashboard in WhiteSource Application Vulnerability Management (AVM) before version 20.4.1 allows Log Injection via

Risk And Classification

Problem Types: CWE-116

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Whitesourcesoftware	Whitesource	All	All	All	All
Application	Whitesourcesoftware	Whitesource	All	All	All	All

References

Reference	Source	Link
WhiteSource Log injection Vulnerability-CVE -2020-5304 by jayaram krishna kumar Medium	MISC	medium.com
WhiteSource Log injection Vulnerability-CVE -2020-5304 by jayaram krishna kumar Medium		medium.com
OSS Security Vulnerabilities Management	MISC	www.whitesourcesoftware.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report