



CVE-2021-21361

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

Summary

CVE	CVE-2021-21361
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-09 01:15:00 UTC
Updated	2021-03-16 18:57:00 UTC
Description	The `com.bmuschko:gradle-vagrant-plugin` Gradle plugin contains an information disclosure vulnerability due to the logging

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vagrant Project	Vagrant	All	All	All	All

References

Reference
Potential credentials leak when setting environmentVariables · Issue #19 · bmuschko/gradle-vagrant-plugin · GitHub
gradle-vagrant-plugin/GDKExternalProcessExecutor.groovy at 292129f9343d00d391543fae06239e9b0f33db73 · bmuschko/gradle-vagrant-pl
Don't print environment by britter · Pull Request #20 · bmuschko/gradle-vagrant-plugin · GitHub
Sensitive information disclosure via log in com.bmuschko:gradle-vagrant-plugin · Advisory · JLLeitschuh/security-research · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982920](#) Java (maven) Security Update for com.bmuschko:gradle-vagrant-plugin (GHSA-jpcm-4485-69p7)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)