Sensitive information disclosure via log in com.bmuschko:gradle-vagrant-plugin

High JLLeitschuh published GHSA-jpcm-4485-69p7 on Mar 8, 2021

Package

com.bmuschko:gradle-vagrant-plugin (Maven)

Affected versions	Patched versions
0.6<, < 3.0.0	3.0.0

Description

Impact

The `com.bmuschko:gradle-vagrant-plugin` Gradle plugin contains an information disclosure vulnerability due to the logging of the system environment variables.

When this Gradle plugin is executed in public CI/CD, this can lead to sensitive credentials being exposed to malicious actors.

Patches

Fixed in version 3.0.0

References

- https://github.com/bmuschko/gradle-vagrant-plugin/blob/292129f9343d00d391543fae06239e9b0f33db73/src/main/groovy/com/bmuschko/gradle/vagrant/process/GDKExternalProcessExecutor.groovy#L42-L44
- bmuschko/gradle-vagrant-plugin#19
- bmuschko/gradle-vagrant-plugin#20

For more information

If you have any questions or comments about this advisory:

- Open an issue in bmuschko/gradle-vagrant-plugin

Severity

High 7.4 / 10

CVSS base metrics	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	None
Availability	None

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

CVE ID

CVE-2021-21361

Weaknesses

CWE-532 CWE-779

Credits

britter