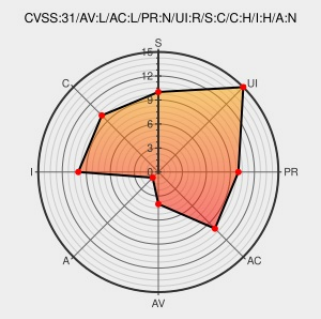
CVE-2020-15167

Published on: 09/02/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 05:45:00 PM UTC

CVE-2020-15167 - advisory for GHSA-mw2v-4q78-j2cw

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Miller from Johnkerl contain the following vulnerability:

In Miller (command line utility) using the configuration file support introduced in version 5.9.0, it is possible for an attacker to cause Miller to run arbitrary code by placing a malicious `.mlrrc` file in the working directory. See linked GitHub Security Advisory for complete details. A fix is ready and will be released as Miller 5.9.1.

CVE-2020-15167 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **johnkerl** - **miller** version **= 5.9.0**

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.4 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Arbitrary code execution via configuration file (.mlrrc) in	Exploit	CONFIRM

working directory · Advisory · johnkerl/miller · GitHub	Third Party Advisory github.com text/html	github.com/johnkerl/miller/security/advisories/GHSA-mw2v-4q78-j2cw

Related QID Numbers

180615 Debian Security Update for miller (CVE-2020-15167)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Johnkerl	Miller	5.9.0	All	All	All
Application	Johnkerl	Miller	5.9.0	All	All	All

cpe:2.3:a:johnkerl:miller:5.9.0:*:*:*:*:*:*:*

cpe:2.3:a:johnkerl:miller:5.9.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→