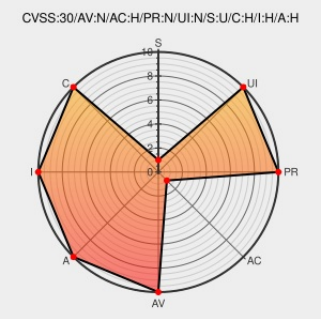
CVE-2019-1010260

Published on: 04/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:56 PM UTC

CVE-2019-1010260

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



Certain versions of Ktlint from Ktlint Project contain the following vulnerability:

Using ktlint to download and execute custom rulesets can result in arbitrary code execution as the served jars can be compromised by a MITM. This attack is exploitable via Man in the Middle of the HTTP connection to the artifact servers. This vulnerability appears to have been fixed in 0.30.0 and later; after commit 5e547b287d6c260d328a2cb658dbe6b7a7ff2261.

CVE-2019-1010260 has been assigned by GSD cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: GSD **ktlint** - **ktlint** version **0.29.0 and earlier [fixed: 0.30.0 and later - after commit 5e547b287d6c260d328a2cb658dbe6b7a7ff2261]**

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[CVE-2019-1010260] [SECURITY] Resolve dependenices over HTTPS instead of HTTP by JLLeitschuh · Pull Request #332 · pinterest/ktlint · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/shyiko/ktlint/pull/332

Related QID Numbers

980892 Java (maven) Security Update for com.github.shyiko.ktlint:ktlint-core (GHSA-r8h9-hq9c-2p5c)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:ktlint_project:ktlint:*:*:*:*:*:*:*:*:

cpe:2.3:a:ktlint_project:ktlint:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→