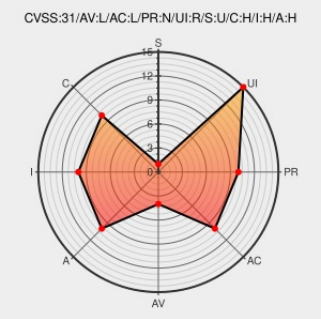
CVE-2020-13651

Published on: 06/15/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-13651

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



Certain versions of Digdash from Digdash contain the following vulnerability:

An issue was discovered in DigDash 2018R2 before p20200528, 2019R1 before p20200421, and 2019R2 before p20200430. It allows a user to provide data that will be used to generate the JNLP file used by a client to obtain the right Java application. By providing an attacker-controlled URL, the client will obtain a rogue JNLP file specifying the installation of malicious JAR archives and executed with full privileges on the client computer.

CVE-2020-13651 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
DigDash Enterprise: Versions 2018R2-2020R1	Third Party Advisory know.bishopfox.com	MISC know.bishopfox.com/advisories/digdash-version-2018

text/html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digdash	Digdash	2018r2	-	All	All
Application	Digdash	Digdash	2019r1	-	All	All
Application	Digdash	Digdash	2019r2	-	All	All
Application	Digdash	Digdash	2018r2	-	All	All
Application	Digdash	Digdash	2019r1	-	All	All
Application	Digdash	Digdash	2019r2	-	All	All

cpe:2.3:a:digdash:digdash:2018r2:-:*:*:*:*:*:*:

cpe:2.3:a:digdash:digdash:2019r1:-:*:*:*:*:*:*:

cpe:2.3:a:digdash:digdash:2019r2:-:*:*:*:*:*:*:

cpe:2.3:a:digdash:digdash:2018r2:-:*:*:*:*:*:*:

cpe:2.3:a:digdash:digdash:2019r1:-:*:*:*:*:*:*:

cpe:2.3:a:digdash:digdash:2019r2:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→