# CVE Detail – CVE-2019-13475

In MobaXterm 11.1, the mobaxterm: URI handler has an argument injection vulnerability that allows remote attackers to execute arbitrary commands when the user visits a specially crafted URL. Based on the available command-line arguments of the software, one can simply inject -exec to execute arbitrary commands. The additional arguments -hideterm and -exitwhendone in the payload make the attack less visible.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.74558

## CVSS Scoring

CVSS v3.0 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')

## CAPEC(s)

* CAPEC-137: Parameter Injection
* CAPEC-174: Flash Parameter Injection
* CAPEC-41: Using Meta-characters in E-mail Headers to Inject Malicious Payloads
* CAPEC-460: HTTP Parameter Pollution (HPP)
* CAPEC-88: OS Command Injection

## Affected Products

* cpe:2.3:a:mobatek:mobaxterm:11.1:\*:\*:\*:\*:\*:\*:\*