# CVE Detail – CVE-2020-26284

Hugo is a fast and Flexible Static Site Generator built in Go. Hugo depends on Go's `os/exec` for certain features, e.g. for rendering of Pandoc documents if these binaries are found in the system `%PATH%` on Windows. In Hugo before version 0.79.1, if a malicious file with the same name (`exe` or `bat`) is found in the current working directory at the time of running `hugo`, the malicious command will be invoked instead of the system one. Windows users who run `hugo` inside untrusted Hugo sites are affected. Users should upgrade to Hugo v0.79.1. Other than avoiding untrusted Hugo sites, there is no workaround.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.60497

## CVSS Scoring

CVSS v3.1 Score: 7.7

Severity: HIGH

## Mapped CWE(s)

* CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

## CAPEC(s)

* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-15: Command Delimiters
* CAPEC-43: Exploiting Multiple Input Interpretation Layers
* CAPEC-6: Argument Injection
* CAPEC-88: OS Command Injection

## Affected Products

* cpe:2.3:a:gohugo:hugo:\*:\*:\*:\*:\*:windows:\*:\*