



# CVE-2019-12554

Published on: 06/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

## CVE-2019-12554

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **010 Editor** from **Sweetscape** contain the following vulnerability:

In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the WSubStr function (provided by the scripting engine) allows an attacker to cause a denial of service by crashing the application.

CVE-2019-12554 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                | Tags                                                                                                                                | Link                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| 010 Editor - Release Notes | <a href="#">Release Notes</a><br><a href="#">Vendor Advisory</a><br><a href="#">www.sweetscape.com</a><br><a href="#">text/html</a> | <b>CONFIRM</b><br><a href="http://www.sweetscape.com/010editor/release_notes.html">www.sweetscape.com/010editor/release_notes.html</a> |

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](mailto: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                                  | Sweetscape | 010 Editor | 9.0.1   | All    | All     | All      |
| Application                                  | Sweetscape | 010 Editor | 9.0.1   | All    | All     | All      |
| cpe:2.3:a:sweetscape:010_editor:9.0.1:*****: |            |            |         |        |         |          |
| cpe:2.3:a:sweetscape:010_editor:9.0.1:*****: |            |            |         |        |         |          |

No vendor comments have been submitted for this CVE