Possible path traversal by use of the `doc` module

Moderate **nilmerg** published **GHSA-cmgc-h4cx-3v43** on Jul 12, 2021

Package

No package listed

Affected versions	Patched versions
2.3.0 to 2.8.2	2.7.5, 2.8.3 and 2.9.0

Description

Impact

The `doc` module of Icinga Web 2 allows to view documentation directly in the UI. It must be enabled manually by an administrator and users need explicit access permission to use it.

Then, by visiting the following route `/icingaweb2/doc/module/image?moduleName=doc&image=../../../../etc/os-release` , it is possible to gain access to arbitrary files readable by the web-server user.

Patches

The issue has been fixed in the v2.7.5, v2.8.3 and v2.9.0 releases.

Workarounds

Disable the `doc` module or revoke permission to use it from all users.

Who Is Affected

If you had already been a victim of this vulnerability can only be verified by inspecting the web server's access log.
Manifestations of such a request in the access log can be identified with this command:

```
grep -Pie '(?<=GET|POST ).+/doc/module/image?(.*image=((\.|%2e)(\.|%2e)(/|%2f)){3,}\S*| )' access.log
```

References

None

Severity

Moderate

CVE ID

CVE-2021-32746

Weaknesses

No CWEs