New issue

Jump to bottom

Possible path traversal when serving static image files #4226

Closed **nilmerg** opened this issue on Aug 14, 2020 · 0 comments · Fixed by #4227

Assignees

Labels area/framework bug queue/important

Milestone 2.8.2

nilmerg commented on Aug 14, 2020 • edited Member

The vulnerability in question allows an attacker to access arbitrary files which are readable by the process running Icinga Web 2. (This is usually the web server or fpm process)

To exploit this vulnerability the attacker has to acquire the following knowledge:

- The URI at which Icinga Web 2 is accessible
- An installed additional (non-core) module, which can be leveraged (Subject to trial-and-error)
- The module's install path (Subject to common knowledge and trial-and-error)

A valid user login is NOT required.

The attack is performed by sending a HTTP GET or POST request to a particular route of Icinga Web 2.
The request has to include the module's name and the desired (relative) file path.

Example:

- Icinga Web 2 is accessible at /icingaweb2
- The business process module is installed and enabled
- The module is installed at /usr/share/icingaweb2/modules

Applicable request to access /etc: "GET /icingaweb2/static/img?module_name=businessprocess&file=../../../../../../etc/os-release"

Since when does it exist?

Since the initial 2.0.0 stable release.

Am I 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 ).+/static/img?(.*file=((\.|%2e)(\.|%2e)(/|%2f)){3,}\S*| )' access.log
```

Which modules can be leveraged?

Known and publicly available modules:

- https://github.com/Icinga/icingaweb2-module-businessprocess
- https://github.com/Icinga/icingaweb2-module-director
- https://github.com/Icinga/icingaweb2-module-reporting
- https://github.com/nbuchwitz/icingaweb2-module-map
- https://github.com/Mikesch-mp/icingaweb2-module-globe

We would like to emphasize that a module itself is **NOT** the cause nor affected. None of the listed modules require a fix in this regard.

nilmerg added bug **TBD** labels on Aug 14, 2020

nilmerg added this to the **2.8.2** milestone on Aug 14, 2020

nilmerg self-assigned this on Aug 14, 2020

nilmerg added **enhancement** and removed bug labels on Aug 14, 2020

nilmerg changed the title ~~Placeholder~~ **Make the world a better place** on Aug 14, 2020

nilmerg added a commit that referenced this issue on Aug 19, 2020

`static/img: Make sure to correctly access module images` ··· `c6baff2`

nilmerg added a commit that referenced this issue on Aug 19, 2020

`static/img: Make sure to correctly access module images` ··· `5700caf`

nilmerg added a commit that referenced this issue on Aug 19, 2020

`static/img: Make sure to correctly access module images` ··· `3035efa`

nilmerg added a commit that referenced this issue on Aug 19, 2020

`static/img: Make sure to correctly access module images` ··· `49d8f49`

nilmerg added **area/framework** bug queue/important and removed **TBD** **enhancement** labels on Aug 19, 2020

nilmerg changed the title ~~Make the world a better place~~ **Possible path traversal when serving static image files** on Aug 19, 2020

nilmerg mentioned this issue on Aug 19, 2020

static/img: Make sure to correctly access module images #4227

Merged

nilmerg closed this as completed in #4227 on Aug 19, 2020

---

bob-beck pushed a commit to openbsd/ports that referenced this issue on Aug 20, 2020

`security update to icinga-web2-2.8.2, possible path traversal when` ··· `d1ff851`

archlinux-github pushed a commit to archlinux/aur that referenced this issue on Aug 2

`new version 2.8.2-1 (security update, fixes CVE-2020-24368)` ··· `445b760`

Assignees

nilmerg

Labels

area/framework bug queue/important

Projects

None yet

Milestone

2.8.2

Development

Successfully merging a pull request may close this issue.

static/img: Make sure to correctly access module images
Icinga/icingaweb2

1 participant