AAA-240

SQL injection in the aaa-idm-store-h2 (deleteDomain function)

Details

Type:	Bug	Status:	RESOLVED
Priority:	Low	Resolution:	Done
Affects Version/s:	0.15.0, (3)	Fix Version/s:	0.17.0, 0.16.5, 0.15.8
Component/s:	None		
Labels:	security		
Environment:	ubuntu20.04, aaa version 0.17.0		

Description

Hello,

I am writing to report a vulnerability in one of the components of Opendaylight, aaa.

With this bug, attackers can SQL inject the component's database(SQLite).

The bug is in /aaa-idm-store-h2/src/main/java/org/opendaylight/aaa/datastore/h2/DomainStore.java (**deleteDomain** function).

As we can see, the aaa concats domainid information to build a delete SQL query, and it executes the query in SQLite.

However, in line 197, the domainid(escaped) is a string. If the user calls the api interface /auth/v1/domains/ to add a malicious domain, and then calls the **deleteDomain** function to delete the domain, it will cause SQL injection.

For example, he can call the api interface /auth/v1/domains/ with POST method, it will call the **createDomain** function to add a domain. If the domain name is:

' or 1=1--+

Then call the api interface /auth/v1/domains/' or 1=1--+ with DELETE method, it will call the **deleteDomain** function to delete the domain. And the SQL query is:

DELETE FROM AAA_DOMAINS WHERE domainid = '' or 1=1—+'

And all the elements in the **AAA_DOMAINS** table are removed due to this malicious query.

Please consider fixing this security vulnerability as soon as possible.

Best wishes,

Chunyang Han

Gerrit Reviews

No reviews matched the request. Check your Options in the drop-down menu of this sections header.

Activity

Filter by: None

Write a comment...

Robert Varga 16/Nov/22 5:26 PM

Thanks for the report, https://git.opendaylight.org/gerrit/c/aaa/+/103242 should take care of this.

People

Assignee:
Robert Varga

Reporter:
Han Chunyang

Votes:
0 Vote for this issue

Watchers:
2 Start watching this issue

Dates

Due:
30/Nov/22

Created:
16/Nov/22 7:07 AM

Updated:
5 hours ago

Resolved:
16/Nov/22 6:06 PM

Time Tracking

Estimated:

	2w
Remaining:	
	4d
Logged:	
	Not Specified