






SQL injection in the aaa-idm-store-h2 (deleteRole 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:	ubuntu22.04, aaa version 0.17.0		
Description			
<p>Hello,</p> <p>I am writing to report a vulnerability in one of the components of Opendaylight, aaa.</p> <p>With this bug, attackers can SQL inject the component's database(SQLite).</p> <p>The bug is in /aaa-idm-store-h2/src/main/java/org/opendaylight/aaa/datastore/h2/RoleStore.java (deleteRole function).</p> <p>As we can see, the aaa concatenates roleid information to build a delete SQL query, and it executes the query in SQLite.</p> <p>However, in line 181, the roleid(escaped) is a string. If the user calls the api interface /auth/v1/roles/ to add a malicious role, and then calls the deleteRole function to delete the role, it will cause SQL injection.</p> <p>For example, he can call the api interface /auth/v1/roles/ with POST method, it will call the createRole function to add a user. If the role name is:</p> <p>* or 1=1--+</p> <p>Then call the api interface /auth/v1/roles/ or 1=1--+@DOMAIN_ID with DELETE method, it will call the deleteRole function to delete the user. And the SQL query is:</p> <p>DELETE FROM AAA_ROLES WHERE roleid = '' or 1=1--+'@DOMAIN_ID</p> <p>And all the elements in the AAA_ROLES table are removed due to this malicious query.</p> <p>Please consider fixing this security vulnerability as soon as possible.</p> <p>Best wishes,</p> <p>Chunyang Han</p>			
Gerrit Reviews			
<p> No reviews matched the request. Check your Options in the drop-down menu of this sections header.</p>			
Activity			
<div>Filter by: None</div> <div>Write a comment...</div>			
<p>Robert Varga 16/Nov/22 5:26 PM</p> <p>Thanks for the report, https://git.opendaylight.org/gerrit/c/aaa/+103241 should take care of this.</p>			
People			
<p>Assignee:</p> <p> Robert Varga</p> <p>Reporter:</p> <p> Han Chunyang</p> <p>Votes:</p> <p>0 Vote for this issue</p> <p>Watchers:</p> <p>2 Start watching this issue</p>			
Dates			
<p>Due:</p> <p>30/Nov/22</p> <p>Created:</p> <p>16/Nov/22 6:51 AM</p> <p>Updated:</p> <p>5 hours ago</p> <p>Resolved:</p> <p>16/Nov/22 6:07 PM</p>			
Time Tracking			
<p>Estimated:</p>			

Remaining:

4d

Logged:

Not Specified