April 24th , 2024

Security Vulnerability Notification (On-premise customers only)

The vulnerability has already been removed from SaaS customers as part of the standard Stibo Systems operating SaaS procedures.

Stibo Systems is sending this notification to you as a vulnerability has been identified in the STEP Software deployment that could expose a TLS private key externally. A man-in-the-middle attack could potentially exploit this vulnerability by allowing decryption and inspection of requests and data transferred between STEP user interfaces/API clients and STEP.

We are not aware of any exploitation of this vulnerability.

The vulnerability is only relevant for customers using HAProxy as a front-end for STEP (not Apache). A hotfix has been created that can be applied without downtime. We strongly encourage all on-premise customers using the HAProxy front-end to apply this hotfix at their earliest convenience.

If you are in doubt whether you are running HAProxy, run the following command on your STEP server:

```
./spot --prop LoadBalancer.Certificate.File | grep File
```

If the output contains the message ***“Found 1 properties matching ‘LoadBalancer.Certificate.File’”*** your deployment is running HAProxy as a frontend, and you should follow the hotfix procedure outlined below.

Hotfix installation procedure.

This command, on the server running the frontend, will install the needed loadbalancer-frontend version and restart HAProxy to use the new configuration created, without affecting the STEP server itself:

```
./spot --hot --apply to:loadbalancer-frontend/7.0/loadbalancer-frontend-7.0.44.spr
```

Please note; “—hot” option tells spot not to stop the STEP app server, this is important if the frontend is co-located with the STEP app server, if the frontend runs on a separate host, then the option does nothing.

Following the hotfix's installation, you must install new TLS certificates. This should be done in order to change the encryption and remediate the case where the vulnerability has already been exploited and the private key extracted.

Testing

To test that the hotfix has successfully been deployed and the HAProxy process has been restarted and using the new configuration, run:

```
curl --verbose -k  https://step.example.com/loadbalancer/test
```

Look for the response “***HTTP/2 403”***

When the curl command is run, the STEP server will log a message starting with: ***"An attempt was made to use the load balancer REST API without a valid key, by a client at ..."***, this message is also a confirmation that the hotfix patching has been deployed successfully and as such is not a real error message.

Please feel free to create an issue on Stibo Service Portal if any further information or assistance is needed. https://service.stibosystems.com/