TykTechnologies / tyk Public

Code Issues 310 Pull requests 112 Actions Projects Security ...

New issue

Jump to bottom

[TT-1397] Security: Path Traversal Bug - Able to delete/modify arbitrary JSON files via management API #3390

Open calabdean opened this issue on Nov 17, 2020 · 1 comment

Labels bug zendesk

calabdean commented on Nov 17, 2020

Branch/Environment/Version

- Branch/Version: https://github.com/TykTechnologies/tyk/tree/v3.0.1
- Environment: On-Prem, Linux

Describe the bug
The function at https://github.com/TykTechnologies/tyk/blob/v3.0.1/gateway/api.go#L771 is able to delete arbitrary JSON files on disk where Tyk is running via the management API. The APIID is provided by the user and this value is then used to create a file on disk. If there is a file found with the same name then it will be deleted and then re-created with the contents of the API creation request.

Assume I create an API with APIID="../../something" - if there is a JSON file at that location called something.json, it will be deleted and replaced with the API definition object from my request.

This means 2 things:

- Actors are able to traverse the file system of the Tyk host
- Actors are able to delete and modify any JSON file on the Tyk host

Reproduction steps

- Create a file outside of where Tyk is storing the API definitions eg ../something.json
- Make a request to create an API with APIID '../something'
- Observe file get deleted and then overwritten

Actual behavior
Tyk deletes/modifies arbitrary JSON files

Expected behavior
Tyk should not use user defined input as part of file names. Recommended that the API gateway maintains a mapping between apiIDs and a gateway generated FileName i.e. a UUID.

Screenshots/Video
N/A

Logs (debug mode or log file):
N/A

Configuration (tyk config file):
N/A

Additional context
N/A

calabdean added the bug label on Nov 17, 2020

buger added the **zendesk** label on Feb 8, 2021

christtyk changed the title ~~Security: Path Traversal Bug - Able to delete/modify arbitrary JSON files via management API~~ **[TT-1397] Security: Path Traversal Bug - Able to delete/modify arbitrary JSON files via management API** on Mar 26, 2021

Moses-oyedeji commented on Jun 28, 2021

@calabdean Thanks for contacting Tyk!
We apologize for the delayed response. The issue is currently being reviewed and we will keep you updated as soon as we can

Assignees
No one assigned

Labels
bug zendesk

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

3 participants