Open Redirect In Jupyter Server

PYTHON OPEN REDIRECT

Yaniv Nizry Dec 17, 2020

Details Overview

Summary

The Jupyter Server provides the backend (i.e. the core services, APIs, and REST endpoints) for Jupyter web applications like Jupyter notebook, JupyterLab, and Voila. Affected versions of Jupyter Server are vulnerable to open redirect vulnerability. All jupyter servers running without a base_url prefix are technically affected, however, these maliciously crafted links can only be reasonably made for known jupyter server hosts.

Product

Jupyter Server before version 1.1.1

Impact

A link to a jupyter server may appear safe, but ultimately redirect to a malicious site.

Steps To Reproduce

1. Run a jupyter server on port 1111
2. Navigate to `http://localhost:1111/login?next=//example.com`

Expected Result:

`https://example.com` will load.

Remediation

Use on of the two options:

1. Update jupyter_server package to 1.1.1 or above.
2. Run your server on a url prefix: "jupyter server --ServerApp.base_url=/jupyter/".

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher Yaniv Nizry.

Resources

1. Advisory
2. Commit 85e4abc