huntr

Open Redirect in archivy/archivy

0

✓ Valid Reported on Feb 16th 2022

Description

The application doesn't check the target website before redirecting leads to Open Redirect vulnerability.

Proof of Concept

Install local service for testing

Step 1: Go to http://127.0.0.1:5000/login?next=%2F%2fevil.com
Step 2: Enter valid credential, you will be redirect to evil.com
PoC: https://drive.google.com/file/d/1mwGtImU2srYZ_3FlHQBrAJFzt3PyZQzM

Impact

Attackers can redirect users to any website and perform phishing attacks.

Occurrences

routes.py L266-L267

CVE
CVE-2022-0697
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Low (3.4)

Visibility
Public

Status

Fixed

Found by

nhiephon

@nhiephon

master

This report was seen 483 times.

We are processing your report and will contact the **archivy** team within 24 hours. 9 months ago

We have contacted a member of the **archivy** team and are waiting to hear back 9 months ago

We have sent a follow up to the **archivy** team. We will try again in 7 days. 9 months ago

A **archivy/archivy** maintainer validated this vulnerability 9 months ago

nhiephon has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

We have sent a fix follow up to the **archivy** team. We will try again in 7 days. 9 months ago

We have sent a second fix follow up to the **archivy** team. We will try again in 10 days. 9 months ago

A **archivy/archivy** maintainer marked this as fixed in **1.7.0** with commit **2d8cb2** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

routes.py#L266-L267 has been validated ✓

Sign in to join this conversation

Chat with us

Chat with us