Web Cache Poisoning

Affecting bottle package, versions [0,0.12.19)

INTRODUCED: 13 OCT 2020 CVE-2020-28473 CWE-444 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `bottle` to version 0.12.19 or higher.

Overview

Affected versions of this package are vulnerable to Web Cache Poisoning by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.

PoC

```
GET /?q=legitimate&utm_content=1;q=malicious HTTP/1.1
Host: example.com

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag e/webp,image/apng,/;q=0.8,application/signed-
exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate


Accept-Language: en-US,en;q=0.9 Connection: close
```

The server sees 3 parameters here: `q`, `utm_content` and then `q` again. On the other hand, the proxy considers this full string: `1;q=malicious` as the value of `utm_content`, which is why the cache key would only contain `somesite.com/?q=legitimate`.

References

- Web Cache Poisoning - Snyk Research Blog

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
User Interaction	Required
Availability	HIGH

See more

SUSE 6.8 MEDIUM

NVD 6.8 MEDIUM

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-PYTHON-BOTTLE-1017108
Published	18 Jan 2021
Disclosed	13 Oct 2020
Credit	Snyk Security Team

Report a new vulnerability | Found a mistake?