CVE-2023-23277

SnippetBox - XSS

CRITICAL

In 2023 Q1 an issue was identified within Snippet-box, an open-source code snippet management system. Versions v1.0.0 and prior versions are vulnerable to a Stored Cross Site Scripting attack, allowing an attacker execute arbitrary webscript (JS, WASM, etc).

Vulnerability Categorisation

Severity: CRITICAL
Vendor: SnippetBox (open-source)
Vulnerability Type: Stored Cross Site Scripting
Attack Type: Remote & Unauthenticated
Impact: Arbitrary WebScript Execution
Attack Vectors: Raw Snippet URL
Affected Component: src/controllers/snippets.ts
Sophistication: Low
Full Disclosure: Vulnerability has not been patched within four months of disclosure.

Zero-Day Exploitation

Exploited In Wild: Unknown
Notes: There have been no public accounts regarding exploitation occurring. However, we are unsure.

Vulnerability Attack Vector

To exploit this vulnerability an attacker must create a new, or edit a existing snippet and set the contents to his webscript payload.
Next the attacker must get a victim to click the “raw url” of the snippet.

```
<script>alert(“Snippet-box XSS“)</script>
```

Affected Component

This vulnerability is caused by src/controllers/snippets.ts’s getRawCode() function not setting the content-type header appropriately. This leads to the browser executing the webpage as “text/html”, allowing for arbitrary webscript execution. This issue can easily be patched by setting the “content-type” header to “text/plain”, further adding the header “x-content-type-options” to “nosniff”.

It is recommended users utilise their load balancer to apply these headers to the route:

```
/api/snippets/raw/*
```

github.com/go-compile April-08-2023