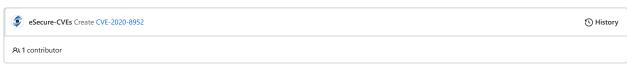


<> Code ⊙ Issues 🏗 Pull requests ⊙ Actions 🖽 Projects ① Security 🗠 Insights

...

CVEs / CVE-2020-8952

ሦ master ▼



```
65 lines (65 sloc) | 1.82 KB
                                                                                                                                             ...
    > Fiserv Accurate Reconciliation 2.19.0 allows XSS via the logout.jsp timeOut parameter.
    > [Additional Information]
    > Capital "R" letters in the payload were used to bypass application layer filtering.
 8 > In the Accurate Reconciliation web application, it was found that
    > attacker-controlled JavaScript could be injected in the timeout logout
    > notification page; resulting in a reflected Cross-Site Scripting (XSS)
11
    > attack.
12
    > Example malicious link:
13
    > https://example.com/accurate/logout.jsp?t=3&timeOut=%3Ca%20hRef=%27javascRipt:alert`XSS`%27%3EClickMe%3C/a%3E
14
    17
    18
    > ------
19
20
    > [Vulnerability Type]
21
    > Cross Site Scripting (XSS)
23
24
    > ------
25
    > [Vendor of Product]
26
27
    > Fiserv, Inc.
 30
31
    > [Affected Product Code Base]
32
    > Accurate Reconciliation - 2.19.0
33
 34
    > [Affected Component]
37
    > Web application (timeout logout notification page)
38
39
    > ------
40
    > [Attack Type]
 42
43
44
    > -----
45
    > [Impact Code execution]
46
    > true
 48
49
    > -----
50
51
    > [Attack Vectors]
    > Reflected Cross Site Scripting (XSS) attacks are delivered to victims
52
    > via direct links. When a user is tricked into clicking on a malicious
    > link, the injected code is reflected in the vulnerable web site, which
55
     > executes client-side code in the user's browser.
56
57
    > ------
58
59
    > [Discoverer]
    > Artem Brunov on behalf of TAL Australia
61
62
63
    > [Reference]
64
    > https://www.esecure.com.au/news
```