eSecure-CVEs / **CVEs** Public

Code Issues Pull requests Actions Projects Security Insights

master

CVEs / CVE-2020-8952

eSecure-CVEs Create CVE-2020-8952 History

1 contributor

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.
>
> 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)
> attack.
>
> Example malicious link:
> https://example.com/accurate/logout.jsp?t=3&amp;timeOut=%3Ca%20hRef=%27javascRipt:alert`XSS`%27%3EClickMe%3C/a%3E
>
> Visiting this link will reflect malicious code which will be executed
> if the victim clicks on the ClickMe link.
>
> ------------------------------------------
>
> [Vulnerability Type]
> Cross Site Scripting (XSS)
>
> ------------------------------------------
>
> [Vendor of Product]
> Fiserv, Inc.
>
> ------------------------------------------
>
> [Affected Product Code Base]
> Accurate Reconciliation - 2.19.0
>
> ------------------------------------------
>
> [Affected Component]
> Web application (timeout logout notification page)
>
> ------------------------------------------
>
> [Attack Type]
> Remote
>
> ------------------------------------------
>
> [Impact Code execution]
> true
>
> ------------------------------------------
>
> [Attack Vectors]
> Reflected Cross Site Scripting (XSS) attacks are delivered to victims
> 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
> executes client-side code in the user's browser.
>
> ------------------------------------------
>
> [Discoverer]
> Artem Brunov on behalf of TAL Australia
>
> ------------------------------------------
>
> [Reference]
> https://www.esecure.com.au/news
```