eSecure-CVEs Create CVE-2020-8951 History

1 contributor

57 lines (57 sloc) | 1.43 KB

```
> Fiserv Accurate Reconciliation 2.19.0 allows XSS via the Source or
> Destination field of the Configuration Manager (Configuration
> Parameter Translation) page.
>
> ----------------------------------------
>
> [Additional Information]
> Capital "R" letters in the payload were used to bypass application layer filtering <scRipt>onerror=alert`XSS`</script>
>
> The payload will be executed each time the affected page is accessed.
>
> ----------------------------------------
>
> [Vulnerability Type]
> Cross Site Scripting (XSS)
>
> ----------------------------------------
>
> [Vendor of Product]
> Fiserv, Inc.
>
> ----------------------------------------
>
> [Affected Product Code Base]
> Accurate Reconciliation - 2.19.0
>
> ----------------------------------------
>
> [Affected Component]
> Web application (Configuration Manager)
>
> ----------------------------------------
>
> [Attack Type]
> Remote
>
> ----------------------------------------
>
> [Impact Code execution]
> true
>
> ----------------------------------------
>
> [Attack Vectors]
> Stored Cross Site Scripting (XSS) attacks are delivered to victims by
> storing payloads within the application which are later executed when
> an unsuspecting user accesses the page.
>
> ----------------------------------------
>
> [Discoverer]
> Artem Brunov on behalf of TAL Australia
>
> ----------------------------------------
>
> [Reference]
> https://www.esecure.com.au/news
```