Mutation XSS In Mozilla-Bleach Via Svg Or Math

PYTHON MOZILLA XSS MXSS

Yaniv Nizry Mar 17, 2020

Details Overview

Summary

Mutation XSS (mXSS) vulnerability in Mozilla-bleach , when RCDATA and either svg or math tags are whitelisted and the keyword argument `strip=False`. It happens due to improper sanitization of the RCDATA tags (`script, noscript, style, noframes, xmp, noembed` and `iframe`) when placed under `svg` or `math`, allowing the browser to execute arbitrary HTML in RCDATA on the victim's browser.

Product

Bleach before 3.1.2

Impact

According to GitHub, more than 72,000 repositories are dependent on Bleach. Among them are major vendors, including multiple Fortune 500 tech companies.

Steps To Reproduce

```
>>> import bleach
>>> bleach.clean('<svg><style><img src=x onerror=alert(1)>', tags=["svg","style"])
```

Expected Result:

`<svg><style><img src=x onerror=alert(1)></style></svg>`

Remediation

Update bleach dependency to 3.1.2 and above

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher Yaniv Nizry.

Resources

1. Blog
2. Advisory
3. Commit 175f677