Mutation XSS In Mozilla-Bleach Via Noscript

PYTHON MOZILLA XSS MXSS

Yaniv Nizry Feb 25, 2020

Details Overview

Summary

Mutation XSS (mXSS) vulnerability in Mozilla-bleach when `noscript` tag is allowed in addition to one of the following tags: `title, textarea, script, style, noembed, noframes, iframe, xmp or comment.`
This occurs due to bleach utilizing its parser, html5lib, with `scripting=False`. In this case, the data of the noscript tags will be parsed as HTML, while the browser parses them as rawdata. This can cause arbitrary HTML and JavaScript codes to run on the victim's browser.

Product

Bleach before 3.1.1

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('<noscript><style></noscript><img src=x onerror=alert(1)>', tags=["noscript","style"])
```

Expected Result:

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

Remediation

Update bleach dependency to 3.1.1 and above

Credit

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

Resources

1. Blog
2. Advisory
3. Commit f77e0f6