# Submit #562301: uBlock @gorhill/ubo-core >=npm_0.1.11 Inefficient Regular Expression Complexity

| | |
|---|---|
| **Title** | **uBlock @gorhill/ubo-core >=npm_0.1.11 Inefficient Regular Expression Complexity** |
| **Description** | A potential Regular Expression Denial of Service (ReDoS)vulnerability in the 1p-filters.js script of uBlock Origin. The vulnerabilityoccurs due to the use of the regular expression /\s+$/, which is used to removetrailing whitespace. This issue can lead to a denial of service when processingstrings with a large number of trailing spaces, potentially causing a browser tofreeze.<br>The regular expression /\s+$/ is applied to remove trailing whitespace in user-provided content. However, when the content has a large number of spaces(e.g., ~100,000), this pattern causes excessive backtracking in the regularexpression engine, resulting in performance degradation and UI freezing. This is a classic ReDoS attack vector. |
| **Source** | ⚠️ https://github.com/gorhill/uBlock/commit/eaedaf5b10d2f7857c6b77fbf7d4a80681d4d46c |
| **User** | 🔒 DayShift (UID 80963) |
| **Submission** | 04/19/2025 10:04 AM (14 days ago) |
| **Moderation** | 05/02/2025 02:53 PM (13 days later) |
| **Status** | Accepted |
| **VulDB Entry** | 307194 [gorhill uBlock Origin up to 1.63.3b16 UI src/js/1p-filters.js currentStateChanged redos] |
| **Points** | 20 |

## ⚠ Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

## Documentation

- Submission Policy
- Data Processing
- CVE Handling