VDB-307194 · CVE-2025-4215 · GCVE-100-307194

GORHILL UBLOCK ORIGIN UP TO 1.63.3B16 UI SRC/JS/1P-FILTERS.JS CURRENTSTATECHANGED REDOS

A vulnerability was found in gorhill uBlock Origin up to 1.63.3b16. It has been classified as problematic. Affected is the function `currentStateChanged` of the file *src/js/1p-filters.js* of the component *UI*. The manipulation with an unknown input leads to a redos vulnerability. CWE is classifying the issue as CWE-1333. The product uses a regular expression with an inefficient, possibly exponential worst-case computational complexity that consumes excessive CPU cycles. This is going to have an impact on availability.

The advisory is available at github.com. This vulnerability is traded as CVE-2025-4215. The exploitability is told to be difficult. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Successful exploitation requires user interaction by the victim. Technical details and a public exploit are known. This vulnerability is assigned to T1449.003 by the MITRE ATT&CK project.

The exploit is shared for download at github.com. It is declared as proof-of-concept.

Upgrading to version 1.63.3b17 eliminates this vulnerability. The upgrade is hosted for download at github.com. Applying the patch eaedaf5b10d2f7857c6b77fbf7d4a80681d4d46c is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

Product

Vendor

- gorhill

Name

- uBlock Origin

Version

- 1.63.3b16

License

- open-source

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 3.1
VulDB Meta Temp Score: 2.9

VulDB Base Score: 3.1
VulDB Temp Score: 2.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 3.1
CNA Vector: 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Redos
CWE: CWE-1333 / CWE-400 / CWE-404
CAPEC: 🔒

ATT&CK: 🔒

Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: uBlock Origin 1.63.3b17
Patch: eaedaf5b10d2f7857c6b77fbf7d4a80681d4d46c

Timeline

05/02/2025		Advisory disclosed
05/02/2025	+0 days	VulDB entry created
05/03/2025	+1 days	VulDB entry last update

Sources

Advisory: eaedaf5b10d2f7857c6b77fbf7d4a80681d4d46c
Status: Confirmed

CVE: CVE-2025-4215 (🔒)
GCVE (CVE): GCVE-0-2025-4215
GCVE (VulDB): GCVE-100-307194
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 05/02/2025 02:58 PM
Updated: 05/03/2025 10:11 AM
Changes: 05/02/2025 02:58 PM (62), 05/03/2025 10:11 AM (30)
Complete: 🔍
Submitter: DayShift
Cache ID: 5:435:101

Submit

Accepted

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

Discussion

No comments yet. Languages: en.

Please log in to comment.