



CVE-2021-36773

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-36773
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-18 04:15:00 UTC
Updated	2023-01-20 02:12:00 UTC
Description	uBlock Origin before 1.36.2 and nMatrix before 4.4.9 support an arbitrary depth of parameter nesting for strict blocking, whi

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Sciruby	Nmatrix	All	All	All	All
Application	Ublockorigin	Ublock Origin	All	All	All	All
Application	Umatrix Project	Umatrix	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3062-1] ublock-origin security update	MLIST	lists.debian.org	
uBlock Origin (and uMatrix) DoS with strict-blocking filter and crafted URL Hacker News	MISC	news.ycombinator.com	
writings/ublock_origin_and_umatrix_denial_of_service.adoc at main · vtriolet/writings · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179482](#) Debian Security Update for ublock-origin (CVE-2021-36773)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)