



CVE-2010-1195

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

Summary

CVE	CVE-2010-1195
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-31 18:00:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in the htmlscrubber component in ikiwiki 2.x before 2.53.5 and 3.x before 3.2010031

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ikiwiki	ikiwiki	2.0	All	All	All

Application	Ikiwiki	Ikiwiki	2.1	All	All	All
Application	Ikiwiki	Ikiwiki	2.10	All	All	All
Application	Ikiwiki	Ikiwiki	2.11	All	All	All
Application	Ikiwiki	Ikiwiki	2.12	All	All	All
Application	Ikiwiki	Ikiwiki	2.13	All	All	All
Application	Ikiwiki	Ikiwiki	2.14	All	All	All
Application	Ikiwiki	Ikiwiki	2.15	All	All	All
Application	Ikiwiki	Ikiwiki	2.16	All	All	All
Application	Ikiwiki	Ikiwiki	2.17	All	All	All
Application	Ikiwiki	Ikiwiki	2.18	All	All	All
Application	Ikiwiki	Ikiwiki	2.19	All	All	All
Application	Ikiwiki	Ikiwiki	2.2	All	All	All
Application	Ikiwiki	Ikiwiki	2.20	All	All	All
Application	Ikiwiki	Ikiwiki	2.3	All	All	All
Application	Ikiwiki	Ikiwiki	2.30	All	All	All
Application	Ikiwiki	Ikiwiki	2.31	All	All	All
Application	Ikiwiki	Ikiwiki	2.31.1	All	All	All
Application	Ikiwiki	Ikiwiki	2.31.2	All	All	All
Application	Ikiwiki	Ikiwiki	2.31.3	All	All	All
Application	Ikiwiki	Ikiwiki	2.4	All	All	All
Application	Ikiwiki	Ikiwiki	2.40	All	All	All
Application	Ikiwiki	Ikiwiki	2.41	All	All	All
Application	Ikiwiki	Ikiwiki	2.42	All	All	All
Application	Ikiwiki	Ikiwiki	2.43	All	All	All
Application	Ikiwiki	Ikiwiki	2.44	All	All	All
Application	Ikiwiki	Ikiwiki	2.45	All	All	All
Application	Ikiwiki	Ikiwiki	2.46	All	All	All
Application	Ikiwiki	Ikiwiki	2.47	All	All	All
Application	Ikiwiki	Ikiwiki	2.48	All	All	All
Application	Ikiwiki	Ikiwiki	2.49	All	All	All
Application	Ikiwiki	Ikiwiki	2.5	All	All	All
Application	Ikiwiki	Ikiwiki	2.50	All	All	All
Application	Ikiwiki	Ikiwiki	2.51	All	All	All
Application	Ikiwiki	Ikiwiki	2.52	All	All	All
Application	Ikiwiki	Ikiwiki	2.53	All	All	All
Application	Ikiwiki	Ikiwiki	3.00	All	All	All

Application	Ikiwiki	Ikiwiki	3.01	All	All	All
Application	Ikiwiki	Ikiwiki	3.02	All	All	All
Application	Ikiwiki	Ikiwiki	3.03	All	All	All
Application	Ikiwiki	Ikiwiki	3.04	All	All	All
Application	Ikiwiki	Ikiwiki	3.05	All	All	All
Application	Ikiwiki	Ikiwiki	3.06	All	All	All
Application	Ikiwiki	Ikiwiki	3.07	All	All	All
Application	Ikiwiki	Ikiwiki	3.08	All	All	All
Application	Ikiwiki	Ikiwiki	3.09	All	All	All
Application	Ikiwiki	Ikiwiki	3.10	All	All	All
Application	Ikiwiki	Ikiwiki	3.11	All	All	All
Application	Ikiwiki	Ikiwiki	3.12	All	All	All
Application	Ikiwiki	Ikiwiki	3.13	All	All	All
Application	Ikiwiki	Ikiwiki	3.14	All	All	All
Application	Ikiwiki	Ikiwiki	3.141	All	All	All
Application	Ikiwiki	Ikiwiki	3.1415	All	All	All
Application	Ikiwiki	Ikiwiki	3.14159	All	All	All
Application	Ikiwiki	Ikiwiki	3.141592	All	All	All
Application	Ikiwiki	Ikiwiki	3.1415926	All	All	All
Application	Ikiwiki	Ikiwiki	3.14159265	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091009	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091017	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091022	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091023	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091031	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091113	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091202	All	All	All
Application	Ikiwiki	Ikiwiki	3.20091218	All	All	All
Application	Ikiwiki	Ikiwiki	3.20100102.3	All	All	All
Application	Ikiwiki	Ikiwiki	3.20100122	All	All	All
Application	Ikiwiki	Ikiwiki	3.20100212	All	All	All
Application	Ikiwiki	Ikiwiki	3.20100302	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CVN	N/A	N/A	affected v/s	Not specified

CVE	NA	N/A	affected n/a	NOT SPECIFIED
References				
Reference	Source	Link		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.v		
Debian update for ikiwiki - Secunia.com	af854a3a-2127-422b-91ae-364da2661108	secun		
ikiwiki "data:image/svg+xml" URI Script Insertion Vulnerability - Advisories - Community	af854a3a-2127-422b-91ae-364da2661108	secun		
Debian -- Security Information -- DSA-2020-1 ikiwiki	af854a3a-2127-422b-91ae-364da2661108	www.c		
security	af854a3a-2127-422b-91ae-364da2661108	ikiwiki.		
CVE Program record	CVE.ORG	www.c		
NVD vulnerability detail	NVD	nvd.ni		
<div style="border: 1px solid #ccc; height: 15px; background-color: #f0f0f0; margin-top: 5px;"></div>				
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				

© 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](#).

Free CVE JSON API [cve.report/api](#)

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