

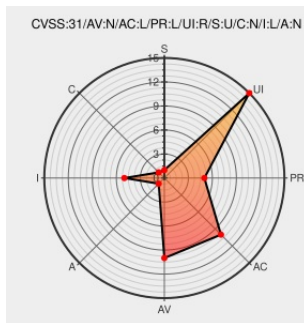


CVE-2020-36525

Published on: Not Yet Published

Last Modified on: 06/11/2022 03:51:00 AM UTC

CVE-2020-36525

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Linking](#) from [Servicerocket](#) contain the following vulnerability:

A vulnerability classified as problematic has been found in Linking. This affects an unknown part of the component New Windows Macro. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.

CVE-2020-36525 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Full Disclosure: SEC Consult SA-20201008-0 :: Multiple Cross-Site Scripting Vulnerabilities in Confluence Marketplace Plugins	seclists.org text/html	MISC seclists.org/fulldisclosure/2020/Oct/15
CVE-2020-36525 Linking New Windows Macro cross site scripting	vuldb.com	MISC vuldb.com/?id=164511

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Servicerocket	Linking	5.5.3	All	All	All
cpe:2.3:a:servicerocket:linking:5.5.3:*:*:*:confluence:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-36525 : A vulnerability classified as problematic has been found in Linking. This affects an unknown part... twitter.com/i/web/status/1...	2022-06-07 18:07:31
 @Festering_Ruin	New vulnerability on the NVD: CVE-2020-36525 June 07, 2022 at 11:15AM ift.tt/fz1dvVI	2022-06-07 20:12:54
 @wvdsteen	New vulnerability on the NVD: CVE-2020-36525 ift.tt/fz1dvVI June 08, 2022 at 06:15AM	2022-06-07 20:16:47
 @workentin	New vulnerability on the NVD: CVE-2020-36525 ift.tt/fz1dvVI	2022-06-07 20:40:28
 @xanadulinux	CVE-2020-36525 ift.tt/fz1dvVI	2022-06-07 20:52:34

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)