



CVE-2021-38614

Published on: 08/12/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:37:00 AM UTC

CVE-2021-38614

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

Certain versions of [Polipo](#) from [Polipo Project](#) contain the following vulnerability:

**** UNSUPPORTED WHEN ASSIGNED **** Polipo through 1.1.1, when NDEBUB is used, allows a heap-based buffer overflow during parsing of a Range header. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2021-38614 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
oss-security - Re: Polipo: denial-of-service using range	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2021/07/28/2

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	Polipo Project	Polipo	All	All	All	All
cpe:2.3:a:polipo_project:polipo:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-38614 : Polipo through 1.1.1, when NDEBUG is used, allows a heap-based buffer overflow during parsing of... twitter.com/i/web/status/1...	2021-08-12 23:04:50

[← Previous ID](#)

[Next ID →](#)