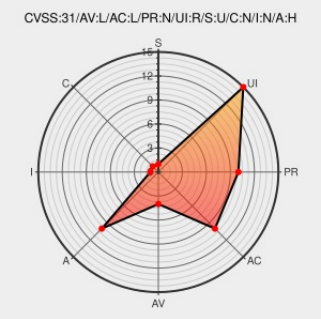
CVE-2015-20109

Published on: Not Yet Published

Last Modified on: 07/31/2023 07:15:00 PM UTC

CVE-2015-20109

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Glibc from Gnu contain the following vulnerability:

end_pattern (called from internal_fnmatch) in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash), as demonstrated by use of the fnmatch library function with the **(!() pattern. NOTE: this is not the same as CVE-2015-8984; also, some Linux distributions have fixed CVE-2015-8984 but have not fixed this additional fnmatch issue.

CVE-2015-20109 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
18036 – buffer overflow (read past end of buffer) in internal_fnmatch=>end_pattern with "**(!()" pattern	sourceware.org text/html	MISC sourceware.org/bugzilla/show_bug.cgi?id=18036
CVE-2015-20109 GNU C Library (glibc) Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20230731-0009/

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	Gnu	Glibc	All	All	All	All

cpe:2.3:a:gnu:glibc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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 registred 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