



CVE-2019-1010025

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

Summary

CVE	CVE-2019-1010025
State	PUBLIC
Assigner	cve-assign@distributedweaknessfiling.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-15 04:15:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	-	All	All	All
Application	Gnu	Glibc	-	All	All	All

References

Reference	Source	Link	Tags
CVE-2019-1010025 Ubuntu	UBUNTU	ubuntu.com	
22853 – (CVE-2019-1010025) Heap address of pthread_create thread is aligned.	MISC	sourceware.org	Exploit, Issue T
support.f5.com/csp/article/K06046097	CONFIRM	support.f5.com	
myF5		support.f5.com	
CVE-2019-1010025	DEBIAN	security-tracker.debian.org	
support.f5.com/csp/article/K06046097	CONFIRM	support.f5.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)