



CVE-2021-3939

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

Summary

CVE	CVE-2021-3939
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-17 04:15:00 UTC
Updated	2023-06-12 07:16:00 UTC
Description	Ubuntu-specific modifications to accountsservice (in patch file debian/patches/0010-set-language.patch) caused the fallback

Risk And Classification

Problem Types: CWE-763

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canonical	Accountsservice	All	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	21.04	All	All	All
Operating System	Canonical	Ubuntu Linux	21.10	All	All	All

References

Reference	Source	Link	Tags
Error: Page not found	MISC	bugs.launchpad.net	
Ubuntu accountsservice Double-Free Memory Corruption ≈ Packet Storm	MISC	packetstormsecurity.com	
USN-5149-1: AccountsService vulnerability Ubuntu security notices Ubuntu	MISC	ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Kevin Backhouse

198573 Ubuntu Security Notification for AccountsService Vulnerability (USN-5149-1)

© [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](#)