



CVE-2021-3709

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

Summary

CVE	CVE-2021-3709
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-01 03:15:00 UTC
Updated	2022-10-27 13:02:00 UTC
Description	Function check_attachment_for_errors() in file data/general-hooks/ubuntu.py could be tricked into exposing private data via

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canonical	Appport	2.14.1-0ubuntu1	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu2	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.1	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.10	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.11	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.12	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.13	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.14	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.15	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.16	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.17	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.18	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.19	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.2	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.20	All	All	All
Application	Canonical	Appport	2.14.1-0ubuntu3.21	All	All	All

Application	Canonical	Apport	2.20.9-0ubuntu7.2	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.20	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.21	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.23	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.24	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.3	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.4	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.5	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.6	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.7	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.8	All	All	All
Application	Canonical	Apport	2.20.9-0ubuntu7.9	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	21.04	All	All	All

References

Reference	Source	Link	Tags
Bug #1934308 "Arbitrary file read in general hook (ubuntu.py)" : Bugs : apport package : Ubuntu	MISC	bugs.launchpad.net	
CVE - CVE-2021-3709	MISC	cve.mitre.org	
USN-5077-1: Apport vulnerabilities Ubuntu security notices Ubuntu	MISC	ubuntu.com	
USN-5077-2: Apport vulnerabilities Ubuntu security notices Ubuntu	MISC	ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

Vendor Comments And Credit

Discovery Credit

LEGACY: Maik Münch (maik@secfault-security.com)(@fktio)

Legacy QID Mappings

198499 Ubuntu Security Notification for Apport Vulnerabilities (USN-5077-1)

© [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](#)