



CVE-2020-27350

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

Summary

CVE	CVE-2020-27350
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-10 04:15:00 UTC
Updated	2022-10-29 02:41:00 UTC
Description	APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in f

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	20.10	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	20.10	All	All	All
Application	Debian	Advanced Package Tool	All	All	All	All
Application	Debian	Advanced Package Tool	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Hardware	Netapp	Solidfire Baseboard Management Controller	-	All	All	All
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All

References

Reference	Source	Link	Tags
-----------	--------	------	------

Debian -- Security Information -- DSA-4808-1 apt	DEBIAN	www.debian.org	Vendc
Bug #1899193 "local denial of service due to parsing bugs in arf...": Bugs : apt package : Ubuntu	CONFIRM	bugs.launchpad.net	Broke
CVE-2020-27350 APT Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
USN-4667-1: APT vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Vendc
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

Vendor Comments And Credit

Discovery Credit

LEGACY: Kevin Backhouse

There are currently no legacy QID mappings associated with this CVE.

© 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