



CVE-2018-12020

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

Summary

CVE	CVE-2018-12020
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-08 21:29:00 UTC
Updated	2022-04-18 17:30:00 UTC
Description	mainproc.c in GnuPG before 2.2.8 mishandles the original filename during decryption and verification actions, which allows

Risk And Classification

Problem Types: CWE-706

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnupg	Gnupg	All	All	All	All
Application	Gnupg	Gnupg	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	Link
USN-3675-3: GnuPG vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com
[Announce] [security fix] GnuPG 2.2.8 released (CVE-2018-12020)	MISC	lists.gnupg.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Debian -- Security Information -- DSA-4224-1 gnupg	DEBIAN	www.debian.org
GnuPG CVE-2018-12020 Security Bypass Vulnerability	BID	www.securityfocus.com
Johnny-You-Are-Fired/johnny-fired.pdf at master · RUB-NDS/Johnny-You-Are-Fired · GitHub	MISC	github.com
⚡ T4012 Diagnostic is shown with the original filename not being sanitized.	MISC	dev.gnupg.org
Debian -- Security Information -- DSA-4222-1 gnupg2	DEBIAN	www.debian.org
DCIM Support	CONFIRM	help.ecostruxureit.com
Red Hat Customer Portal	REDHAT	access.redhat.com

Hed Hat Customer Portal	REDHAT	access.redhat.com
oss-security - CVE-2018-12020 in GnuPG	MISC	openwall.com
GitHub - RUB-NDS/Johnny-You-Are-Fired: Artifacts for the USENIX publication.	MISC	github.com
oss-security - Spoofing OpenPGP and S/MIME Signatures in Emails (multiple clients)	MLIST	www.openwall.com
[SECURITY] [DLA 2862-1] python-gnupg security update	MLIST	lists.debian.org
Johnny You Are Fired ≈ Packet Storm	MISC	packetstormsecurity.com
GnuPG Filename Input Validation Flaw Lets Remote Users Spoof Status Messages - SecurityTracker	SECTRACK	www.securitytracker.com
USN-3675-1: GnuPG vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
Full Disclosure: OpenPGP and S/MIME signature forgery attacks in multiple email clients	FULLDISC	seclists.org
USN-3675-2: GnuPG 2 vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com
Debian -- Security Information -- DSA-4223-1 gnupg1	DEBIAN	www.debian.org
USN-3964-1: python-gnupg vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178969](#) Debian Security Update for python-gnupg (DLA 2862-1)

[500230](#) Alpine Linux Security Update for gnupg

[500358](#) Alpine Linux Security Update for gnupg1

[503976](#) Alpine Linux Security Update for gnupg

© [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](#)