



# CVE-2020-25125

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

## Summary

<b>CVE</b>	CVE-2020-25125
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-03 18:15:00 UTC
<b>Updated</b>	2020-09-11 13:49:00 UTC
<b>Description</b>	GnuPG 2.2.21 and 2.2.22 (and Gpg4win 3.1.12) has an array overflow, leading to a crash or possibly unspecified other imp

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	2.2.21	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	2.2.22	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	2.2.21	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	2.2.22	All	All	All
Application	<a href="#">Gpg4win</a>	<a href="#">Gpg4win</a>	3.1.12	All	All	All
Application	<a href="#">Gpg4win</a>	<a href="#">Gpg4win</a>	3.1.12	All	All	All

## References

Reference	Source	Link
oss-security - GNUPG released with AEAD sec fix CVE-2020-25125	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
oss-security - CVE-2020-25125: gnupg2: buffer overflow when importing a key with AEAD preferences	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Bug 1176034 – VUL-0: CVE-2020-25125: gpg2: AEAD preference list overflow	MISC	<a href="http://bugzilla.opensuse.org">bugzilla.opensuse.org</a>
⚡ T5050 AEAD preference list overflow in 2.2	MISC	<a href="http://dev.gnupg.org">dev.gnupg.org</a>
[Announce] [security fix] GnuPG 2.2.23 released	MISC	<a href="http://lists.gnupg.org">lists.gnupg.org</a>
rG8ec9573e5786	MISC	<a href="http://dev.gnupg.org">dev.gnupg.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[500229](#) Alpine Linux Security Update for gnupg

[503974](#) Alpine Linux Security Update for gnupg

[671538](#) EulerOS Security Update for gnupg2 (EulerOS-SA-2022-1505)

[671540](#) EulerOS Security Update for gnupg2 (EulerOS-SA-2022-1486)

[690473](#) Free Berkeley Software Distribution (FreeBSD) Security Update for gnupg (f9fa7adc-ee51-11ea-a240-002590acae31)

© [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](#)