



# CVE-2022-34903

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-34903
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-01 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:48:00 UTC
<b>Description</b>	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring

## Risk And Classification

### Problem Types: CWE-74

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All

## References

Reference	Source	Link	Ta
[SECURITY] Fedora 35 Update: gnupg2-2.3.4-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 35 Update: gnupg2-2.3.4-2.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: gnupg1-1.4.23-18.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
oss-security - GnuPG signature spoofing via status line injection	MISC	<a href="https://www.openwall.com">www.openwall.com</a>	
[SECURITY] Fedora 35 Update: gnupg1-1.4.23-18.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
#1014157 - gnupg: vulnerable to status injection - Debian Bug report logs	MISC	<a href="https://bugs.debian.org">bugs.debian.org</a>	
[SECURITY] Fedora 36 Update: gnupg2-2.3.6-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	

oss-security - Re: GnuPG signature spoofing via status line injection	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
CVE-2022-34903 GnuPG Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="http://security.netapp.com">security.netapp.com</a>	
[SECURITY] Fedora 36 Update: gnupg1-1.4.23-18.fc36 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: gnupg2-2.3.6-2.fc36 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 35 Update: gnupg1-1.4.23-18.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Debian -- Security Information -- DSA-5174-1 gnupg2	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
⌘ T6027 Revisit write_status_text_and buffer	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>	ca
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[160085](#) Oracle Enterprise Linux Security Update for gnupg2 (ELSA-2022-6463)

[160102](#) Oracle Enterprise Linux Security Update for gnupg2 (ELSA-2022-6602)

[180606](#) Debian Security Update for gnupg2 (DSA 5174-1)

[184489](#) Debian Security Update for gnupg2 (CVE-2022-34903)

[198848](#) Ubuntu Security Notification for GnuPG Vulnerability (USN-5503-1)

[240658](#) Red Hat Update for gnupg2 (RHSA-2022:6463)

[240683](#) Red Hat Update for gnupg2 (RHSA-2022:6602)

[282905](#) Fedora Security Update for gnupg2 (FEDORA-2022-aa14d396dd)

[282962](#) Fedora Security Update for gnupg2 (FEDORA-2022-1124e5882d)

[282977](#) Fedora Security Update for gnupg1 (FEDORA-2022-0dbfb7e270)

[282978](#) Fedora Security Update for gnupg1 (FEDORA-2022-1747eea46c)

[354043](#) Amazon Linux Security Advisory for gnupg2 : ALAS2-2022-1834

[354048](#) Amazon Linux Security Advisory for gnupg2 : ALAS-2022-1630

[354361](#) Amazon Linux Security Advisory for gnupg2 : ALAS2022-2022-207

[354374](#) Amazon Linux Security Advisory for gnupg2 : ALAS2022-2022-126

[354640](#) Amazon Linux Security Advisory for gnupg2 : AL2012-2022-372

[355206](#) Amazon Linux Security Advisory for gnupg2 : ALAS2023-2023-087

[502412](#) Alpine Linux Security Update for gnupg

502414 Alpine Linux Security Update for gnupg
502417 Alpine Linux Security Update for gnupg
503975 Alpine Linux Security Update for gnupg
672095 EulerOS Security Update for gnupg2 (EulerOS-SA-2022-2287)
672116 EulerOS Security Update for gnupg2 (EulerOS-SA-2022-2316)
672190 EulerOS Security Update for gnupg2 (EulerOS-SA-2022-2460)
672264 EulerOS Security Update for gnupg2 (EulerOS-SA-2022-2649)
672270 EulerOS Security Update for gnupg2 (EulerOS-SA-2022-2681)
672323 EulerOS Security Update for gnupg2 (EulerOS-SA-2022-2709)
752377 SUSE Enterprise Linux Security Update for gpg2 (SUSE-SU-2022:2529-1)
752386 SUSE Enterprise Linux Security Update for gpg2 (SUSE-SU-2022:2546-1)
752563 SUSE Enterprise Linux Security Update for gpg2 (SUSE-SU-2022:3144-1)
902450 Common Base Linux Mariner (CBL-Mariner) Security Update for gnupg2 (10077)
902452 Common Base Linux Mariner (CBL-Mariner) Security Update for gnupg2 (10074)
903894 Common Base Linux Mariner (CBL-Mariner) Security Update for gnupg2 (10074-1)
906967 Common Base Linux Mariner (CBL-Mariner) Security Update for gnupg2 (10077-1)
940663 AlmaLinux Security Update for gnupg2 (ALSA-2022:6463)
940682 AlmaLinux Security Update for gnupg2 (ALSA-2022:6602)
960241 Rocky Linux Security Update for gnupg2 (RLSA-2022:6463)
960576 Rocky Linux Security Update for gnupg2 (RLSA-2022:6602)

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)