



CVE-2013-4402

Published on: 10/28/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:27 PM UTC

CVE-2013-4402

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The compressed packet parser in GnuPG 1.4.x before 1.4.15 and 2.0.x before 2.0.22 allows remote attackers to cause a denial of service (infinite recursion) via a crafted OpenPGP message.

CVE-2013-4402 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

Bug 1015685 – CVE-2013-4402 GnuPG: infinite recursion in the compressed packet parser DoS

[bugzilla.redhat.com](https://bugzilla.redhat.com/text/html)
[text/html](#)

CONFIRM
bugzilla.redhat.com/show_bug.cgi?id=1015685

[Announce] [security fix] GnuPG 1.4.15 released

[Vendor Advisory](https://lists.gnupg.org/text/html)
[lists.gnupg.org](#)
[text/html](#)

MLIST [Gnupg-announce] 20131005
[Announce] [security fix] GnuPG 1.4.15 released

#725433 - CVE-2013-4402: infinite recursion in the compressed packet parser - Debian Bug report logs

[bugs.debian.org](https://bugs.debian.org/text/html)
[text/html](#)

CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=725433

Debian -- Security Information -- DSA-2774-1 gnupg2

[www.debian.org](https://www.debian.org/Deprecated Link)
Deprecated Link
[text/html](#)

DEBIAN DSA-2774

openSUSE-SU-2013:1552-1: moderate: gpg2: fixed a denial of service attac

[lists.opensuse.org](https://lists.opensuse.org/text/html)
[text/html](#)

SUSE openSUSE-SU-2013:1552

Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1459
openSUSE-SU-2013:1546-1: moderate: gpg2: fixed a denial of service attac	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1546
Debian -- Security Information -- DSA-2773-1 gnupg	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2773
USN-1987-1: GnuPG vulnerabilities Ubuntu	Vendor Advisory www.ubuntu.com text/html	 UBUNTU USN-1987-1
[Announce] [security fix] GnuPG 2.0.22 released	Vendor Advisory lists.gnupg.org text/html	 MLIST [Gnupg-announce] 20131005 [Announce] [security fix] GnuPG 2.0.22 released
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Application	Gnupg	Gnupg	1.4.0	All	All	All
Application	Gnupg	Gnupg	1.4.10	All	All	All
Application	Gnupg	Gnupg	1.4.11	All	All	All
Application	Gnupg	Gnupg	1.4.12	All	All	All
Application	Gnupg	Gnupg	1.4.13	All	All	All

Application	Gnupg	Gnupg	1.4.14	All	All	All
Application	Gnupg	Gnupg	1.4.2	All	All	All
Application	Gnupg	Gnupg	1.4.3	All	All	All
Application	Gnupg	Gnupg	1.4.4	All	All	All
Application	Gnupg	Gnupg	1.4.5	All	All	All
Application	Gnupg	Gnupg	1.4.8	All	All	All
Application	Gnupg	Gnupg	2.0	All	All	All
Application	Gnupg	Gnupg	2.0.1	All	All	All
Application	Gnupg	Gnupg	2.0.10	All	All	All
Application	Gnupg	Gnupg	2.0.11	All	All	All
Application	Gnupg	Gnupg	2.0.12	All	All	All
Application	Gnupg	Gnupg	2.0.13	All	All	All
Application	Gnupg	Gnupg	2.0.14	All	All	All
Application	Gnupg	Gnupg	2.0.15	All	All	All
Application	Gnupg	Gnupg	2.0.16	All	All	All
Application	Gnupg	Gnupg	2.0.17	All	All	All
Application	Gnupg	Gnupg	2.0.18	All	All	All
Application	Gnupg	Gnupg	2.0.19	All	All	All
Application	Gnupg	Gnupg	2.0.20	All	All	All
Application	Gnupg	Gnupg	2.0.21	All	All	All
Application	Gnupg	Gnupg	1.4.0	All	All	All
Application	Gnupg	Gnupg	1.4.10	All	All	All
Application	Gnupg	Gnupg	1.4.11	All	All	All
Application	Gnupg	Gnupg	1.4.12	All	All	All
Application	Gnupg	Gnupg	1.4.13	All	All	All
Application	Gnupg	Gnupg	1.4.14	All	All	All
Application	Gnupg	Gnupg	1.4.2	All	All	All
Application	Gnupg	Gnupg	1.4.3	All	All	All
Application	Gnupg	Gnupg	1.4.4	All	All	All
Application	Gnupg	Gnupg	1.4.5	All	All	All
Application	Gnupg	Gnupg	1.4.8	All	All	All
Application	Gnupg	Gnupg	2.0	All	All	All
Application	Gnupg	Gnupg	2.0.1	All	All	All
Application	Gnupg	Gnupg	2.0.10	All	All	All
Application	Gnupg	Gnupg	2.0.11	All	All	All

Application	Gnupg	Gnupg	2.0.12	All	All	All
Application	Gnupg	Gnupg	2.0.13	All	All	All
Application	Gnupg	Gnupg	2.0.14	All	All	All
Application	Gnupg	Gnupg	2.0.15	All	All	All
Application	Gnupg	Gnupg	2.0.16	All	All	All
Application	Gnupg	Gnupg	2.0.17	All	All	All
Application	Gnupg	Gnupg	2.0.18	All	All	All
Application	Gnupg	Gnupg	2.0.19	All	All	All
Application	Gnupg	Gnupg	2.0.20	All	All	All
Application	Gnupg	Gnupg	2.0.21	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.0:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.10:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.11:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.12:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.13:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.14:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.2:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.3:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.4:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.5:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:1.4.8:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:2.0:*:*:*:*:*:						
cpe:2.3:a:gnupg:gnupg:2.0.1:*:*:*:*:*:						

cpe:2.3:a:gnupg:gnupg:2.0.10:*****:
cpe:2.3:a:gnupg:gnupg:2.0.11:*****:
cpe:2.3:a:gnupg:gnupg:2.0.12:*****:
cpe:2.3:a:gnupg:gnupg:2.0.13:*****:
cpe:2.3:a:gnupg:gnupg:2.0.14:*****:
cpe:2.3:a:gnupg:gnupg:2.0.15:*****:
cpe:2.3:a:gnupg:gnupg:2.0.16:*****:
cpe:2.3:a:gnupg:gnupg:2.0.17:*****:
cpe:2.3:a:gnupg:gnupg:2.0.18:*****:
cpe:2.3:a:gnupg:gnupg:2.0.19:*****:
cpe:2.3:a:gnupg:gnupg:2.0.20:*****:
cpe:2.3:a:gnupg:gnupg:2.0.21:*****:
cpe:2.3:a:gnupg:gnupg:1.4.0:*****:
cpe:2.3:a:gnupg:gnupg:1.4.10:*****:
cpe:2.3:a:gnupg:gnupg:1.4.11:*****:
cpe:2.3:a:gnupg:gnupg:1.4.12:*****:
cpe:2.3:a:gnupg:gnupg:1.4.13:*****:
cpe:2.3:a:gnupg:gnupg:1.4.14:*****:
cpe:2.3:a:gnupg:gnupg:1.4.2:*****:
cpe:2.3:a:gnupg:gnupg:1.4.3:*****:
cpe:2.3:a:gnupg:gnupg:1.4.4:*****:
cpe:2.3:a:gnupg:gnupg:1.4.5:*****:
cpe:2.3:a:gnupg:gnupg:1.4.8:*****:
cpe:2.3:a:gnupg:gnupg:2.0:*****:
cpe:2.3:a:gnupg:gnupg:2.0.1:*****:
cpe:2.3:a:gnupg:gnupg:2.0.10:*****:
cpe:2.3:a:gnupg:gnupg:2.0.11:*****:
cpe:2.3:a:gnupg:gnupg:2.0.12:*****:

cpe:2.3:a:gnupg:gnupg:2.0.13:*****:
cpe:2.3:a:gnupg:gnupg:2.0.14:*****:
cpe:2.3:a:gnupg:gnupg:2.0.15:*****:
cpe:2.3:a:gnupg:gnupg:2.0.16:*****:
cpe:2.3:a:gnupg:gnupg:2.0.17:*****:
cpe:2.3:a:gnupg:gnupg:2.0.18:*****:
cpe:2.3:a:gnupg:gnupg:2.0.19:*****:
cpe:2.3:a:gnupg:gnupg:2.0.20:*****:
cpe:2.3:a:gnupg:gnupg:2.0.21:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)