



# CVE-2014-3985

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2014-3985
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-09-11 18:55:00 UTC
<b>Updated</b>	2020-09-28 14:57:00 UTC
<b>Description</b>	The getHTTPResponse function in miniwget.c in MiniUPnP 1.9 allows remote attackers to cause a denial of service (crash)

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Miniupnp Project</a>	<a href="#">Miniupnp</a>	1.9	All	All	All
Application	<a href="#">Miniupnp Project</a>	<a href="#">Miniupnp</a>	1.9	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All

## References

Reference	Source	Link	Tags
Bug 1085618 – CVE-2014-3985 miniupnpc buffer overrun - network facing DoS crash	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking
MiniUPnPc: Buffer overflow (GLSA 201701-41) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	Third Party Ac
openSUSE-SU-2014:0815-1: moderate: miniupnpc: Update to 1.9 to fix buffe	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, T
MiniUPnP 'miniwget.c' Remote Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Ac
oss-sec: Re: CVE request: possible miniupnpc buffer overflow	MLIST	<a href="http://seclists.org">seclists.org</a>	Exploit, Mailin
miniwget.c: fixed potential buffer overrun · miniupnp/miniupnp@3a87aa2 · GitHub	CONFIRM	<a href="http://github.com">github.com</a>	Patch, Third P
oss-sec: CVE request: possible miniupnpc buffer overflow	MLIST	<a href="http://seclists.org">seclists.org</a>	Exploit, Mailin
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

710421 Gentoo Linux MiniUPnPc Buffer overflow Vulnerability (GLSA 201701-41)

© [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](#)