



CVE-2015-6031

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

Summary

CVE	CVE-2015-6031
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-02 19:59:00 UTC
Updated	2019-06-18 12:13:00 UTC
Description	Buffer overflow in the IGDstartelt function in igd_desc_parse.c in the MiniUPnP client (aka MiniUPnPc) before 1.9.20150911

Risk And Classification

Problem Types: CWE-119

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	15.04	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	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Miniupnp Project	Miniupnpc	1.9	2014-02-03	All	All
Application	Miniupnp Project	Miniupnpc	1.9	2014-02-05	All	All
Application	Miniupnp Project	Miniupnpc	1.9	2014-05-15	All	All
Application	Miniupnp Project	Miniupnpc	1.9	2014-06-10	All	All
Application	Miniupnp Project	Miniupnpc	1.9	2014-07-01	All	All
Application	Miniupnp Project	Miniupnpc	1.9	2014-09-06	All	All
Application	Miniupnp Project	Miniupnpc	1.9	2014-09-11	All	All

Application	Miniupnp Project	Miniupnpc	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

References

Reference	Source	Link	Tags
USN-2780-2: MiniUPnP vulnerability Ubuntu	UBUNTU	www.ubuntu.com	Third Party Advisory
MiniUPnPc: Arbitrary code execution (GLSA 201801-08) — Gentoo Security	GENTOO	security.gentoo.org	Third Party Advisory
miniupnp/Changelog.txt at master · miniupnp/miniupnp · GitHub	CONFIRM	github.com	Third Party Advisory
openSUSE-SU-2015:2070-1: moderate: Security update for miniupnpc	SUSE	lists.opensuse.org	Mailing List, Third Party Advisory
Cisco Talos - Talos 2015 0035	MISC	talosintel.com	Exploit
Debian -- Security Information -- DSA-3379-1 miniupnpc	DEBIAN	www.debian.org	Third Party Advisory
igd_desc_parse.c: fix buffer overflow · miniupnp/miniupnp@79cca97 · GitHub	CONFIRM	github.com	Third Party Advisory
MiniUPnP 'igd_desc_parse.c' Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory, Vulnerability
USN-2780-1: MiniUPnP vulnerability Ubuntu	UBUNTU	www.ubuntu.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710235](#) Gentoo Linux MiniUPnPc Arbitrary code execution Vulnerability (GLSA 201801-08)

© [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