



# CVE-2004-0461

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

## Summary

<b>CVE</b>	CVE-2004-0461
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-08-06 04:00:00 UTC
<b>Updated</b>	2017-07-11 01:30:00 UTC
<b>Description</b>	The DHCP daemon (DHCPD) for ISC DHCP 3.0.1rc12 and 3.0.1rc13, when compiled in environments that do not provide t

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Infoblox</a>	<a href="#">Dns One Appliance</a>	2.3.1_r5	All	All	All
Hardware	<a href="#">Infoblox</a>	<a href="#">Dns One Appliance</a>	2.4.0.8	All	All	All
Hardware	<a href="#">Infoblox</a>	<a href="#">Dns One Appliance</a>	2.4.0.8a	All	All	All
Hardware	<a href="#">Infoblox</a>	<a href="#">Dns One Appliance</a>	2.3.1_r5	All	All	All
Hardware	<a href="#">Infoblox</a>	<a href="#">Dns One Appliance</a>	2.4.0.8	All	All	All
Hardware	<a href="#">Infoblox</a>	<a href="#">Dns One Appliance</a>	2.4.0.8a	All	All	All
Application	<a href="#">Isc</a>	<a href="#">Dhcpd</a>	3.0.1	rc12	All	All
Application	<a href="#">Isc</a>	<a href="#">Dhcpd</a>	3.0.1	rc13	All	All
Application	<a href="#">Isc</a>	<a href="#">Dhcpd</a>	3.0.1	rc12	All	All
Application	<a href="#">Isc</a>	<a href="#">Dhcpd</a>	3.0.1	rc13	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	amd64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.1	All	ppc	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.2	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.2	All	amd64	All

Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	9.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.1	All	ppc	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	amd64	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Application	Suse	Suse Email Server	iii	All	All	All
Application	Suse	Suse Email Server	iii	All	All	All
Operating System	Suse	Suse Linux	7	All	enterprise_server	All
Operating System	Suse	Suse Linux	8	All	enterprise_server	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.0	All	i386	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Operating System	Suse	Suse Linux	7	All	enterprise_server	All
Operating System	Suse	Suse Linux	8	All	enterprise_server	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.0	All	i386	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Application	Suse	Suse Linux Admin-cd For Firewall	All	All	All	All
Application	Suse	Suse Linux Admin-cd For Firewall	All	All	All	All
Application	Suse	Suse Linux Connectivity Server	All	All	All	All
Application	Suse	Suse Linux Connectivity Server	All	All	All	All
Application	Suse	Suse Linux Database Server	All	All	All	All
Application	Suse	Suse Linux Database Server	All	All	All	All

Application	<a href="#">Suse</a>	<a href="#">Suse Linux Firewall Cd</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Firewall Cd</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Office Server</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Office Server</a>	All	All	All	All

## References

Reference	Source	Link
20040622 DHCP Vuln // no code 0day //	BUGTRAQ	<a href="#">marc.info</a>
US-CERT Vulnerability Note VU#654390	CERT-VN	<a href="#">www.kb.cert.org</a>
'[OpenPKG-SA-2004.031] OpenPKG Security Advisory (dhcpcd)' - MARC	BUGTRAQ	<a href="#">marc.info</a>
XEROX WorkCentre Products Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	<a href="#">secunia.com</a>
US-CERT Technical Cyber Security Alert TA04-174A -- Multiple Vulnerabilities in ISC DHCP 3	CERT	<a href="#">www.us-cert.gov</a>
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.co</a>
<a href="#">www.xerox.com/downloads/usa/en/c/cert_XRX06_004_v11.pdf</a>	CONFIRM	<a href="#">www.xerox.com</a>
Security Announcement	SUSE	<a href="#">www.novell.com</a>
20040628 ISC DHCP overflows	BUGTRAQ	<a href="#">marc.info</a>
Advisories - Mandriva	MANDRAKE	<a href="#">www.mandriva.com</a>
ISC DHCPD VSPRINTF Buffer Overflow Vulnerability	BID	<a href="#">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)