



# CVE-2006-6870

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

## Summary

<b>CVE</b>	CVE-2006-6870
<b>State</b>	PUBLIC
<b>Assigner</b>	security@ubuntu.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-12-31 05:00:00 UTC
<b>Updated</b>	2011-03-08 02:47:00 UTC
<b>Description</b>	The consume_labels function in avahi-core/dns.c in Avahi before 0.6.16 allows remote attackers to cause a denial of service

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avahi	Avahi	0.6.10	All	All	All
Application	Avahi	Avahi	0.6.11	All	All	All
Application	Avahi	Avahi	0.6.12	All	All	All
Application	Avahi	Avahi	0.6.13	All	All	All
Application	Avahi	Avahi	0.6.14	All	All	All
Application	Avahi	Avahi	0.6.15	All	All	All
Application	Avahi	Avahi	0.6.7	All	All	All
Application	Avahi	Avahi	0.6.8	All	All	All
Application	Avahi	Avahi	0.6.9	All	All	All
Application	Avahi	Avahi	0.6.10	All	All	All
Application	Avahi	Avahi	0.6.11	All	All	All
Application	Avahi	Avahi	0.6.12	All	All	All
Application	Avahi	Avahi	0.6.13	All	All	All
Application	Avahi	Avahi	0.6.14	All	All	All
Application	Avahi	Avahi	0.6.15	All	All	All
Application	Avahi	Avahi	0.6.7	All	All	All
Application	Avahi	Avahi	0.6.8	All	All	All

Application	Avahi	Avahi	0.6.9	All	All	All
References						
Reference	Source	Link	Tags			
USN-402-1: Avahi vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>				
Webmail - OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>				
Fedora update for Avahi - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>				
Avahi Compressed DNS Denial Of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>				
#84 (potential endless loop) - Avahi - Trac	CONFIRM	<a href="http://www.avahi.org">www.avahi.org</a>	Patch			
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>				
404 Not Found	FEDORA	<a href="http://fedoraneews.org">fedoraneews.org</a>				
404 Not Found	FEDORA	<a href="http://fedoraneews.org">fedoraneews.org</a>				
Avahi - Trac	CONFIRM	<a href="http://www.avahi.org">www.avahi.org</a>	Patch			
Fedora update for avahi - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>				
404 Not Found	CONFIRM	<a href="http://www.avahi.org">www.avahi.org</a>				
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>				
Avahi "consume_labels()" Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>				
Advisories - Mandriva Linux	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>				
Ubuntu update for avahi - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>				
Mandriva update for avahi - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>				
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical			
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis			

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)