



# CVE-2011-4315

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

## Summary

<b>CVE</b>	CVE-2011-4315
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-12-08 20:55:00 UTC
<b>Updated</b>	2021-11-10 15:54:00 UTC
<b>Description</b>	Heap-based buffer overflow in compression-pointer processing in core/nginx_resolver.c in nginx before 1.0.10 allows remote

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Nginx	All	All	All	All
Application	F5	Nginx	All	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Suse	Studio	1.2	All	All	All
Application	Suse	Studio	1.2	All	All	All
Application	Suse	Studio Onsite	1.2	All	All	All
Application	Suse	Studio Onsite	1.2	All	All	All
Application	Suse	Webyast	1.2	All	All	All
Application	Suse	Webyast	1.2	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] SUSE-SU-2011:1300-1: important: Security update for	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party

Changeset 4268:25ddf6afc0ff – nginx	CONFIRM	<a href="https://trac.nginx.org">trac.nginx.org</a>	Issue Tracking, Patch, Vendor
oss-security - Re: CVE Request: nginx resolver heap overflow	MLIST	<a href="https://openwall.com">openwall.com</a>	Mailing List, Patch, Third Party
<a href="https://www.nginx.org/en/CHANGES-1.0">www.nginx.org/en/CHANGES-1.0</a>	CONFIRM	<a href="https://www.nginx.org">www.nginx.org</a>	Release Notes, Vendor
[SECURITY] Fedora 16 Update: nginx-1.0.10-1.fc16	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Third Party Advisory
nginx DNS Resolver Remote Heap Buffer Overflow Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, Vendor
About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Third Party Advisory
Gentoo Linux Documentation -- nginx: Multiple vulnerabilities	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Party Advisory
Security Alerts - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Third Party Advisory
oss-security - CVE Request: nginx resolver heap overflow	MLIST	<a href="https://openwall.com">openwall.com</a>	Mailing List, Patch, Third Party
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

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