



# CVE-2013-4547

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

## Summary

<b>CVE</b>	CVE-2013-4547
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-11-23 18:55:00 UTC
<b>Updated</b>	2021-11-10 15:59:00 UTC
<b>Description</b>	nginx 0.8.41 through 1.4.3 and 1.5.x before 1.5.7 allows remote attackers to bypass intended restrictions via an unescaped

## Risk And Classification

**Problem Types:** CWE-116

## 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
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Application	Suse	Lifecycle Management Server	1.3	All	All	All
Application	Suse	Lifecycle Management Server	1.3	All	All	All
Application	Suse	Studio Onsite	1.3	All	All	All
Application	Suse	Studio Onsite	1.3	All	All	All

Application	<a href="#">Suse</a>	<a href="#">Webyast</a>	1.3	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Webyast</a>	1.3	All	All	All

## References

Reference	Source	Link	Tags
openSUSE-SU-2013:1792-1: moderate: nginx: fixed restriction bypass probl	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party Advi
About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Third Party Advisory
openSUSE-SU-2013:1745-1: moderate: nginx: fixed restriction bypass probl	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party Advi
Debian -- Page not found	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Broken Link
[security-announce] SUSE-SU-2013:1895-1: important: Security update for	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party Advi
openSUSE-SU-2013:1791-1: moderate: nginx-1.0: fixed restriction bypass p	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party Advi
About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Third Party Advisory
[nginx-announce] nginx security advisory (CVE-2013-4547)	MLIST	<a href="https://mailman.nginx.org">mailman.nginx.org</a>	Mitigation, Vendor Advisory
About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Third Party Advisory
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](#) 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](https://status.cve.report)