CVE-2011-4315

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2011-4315
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-12-08 20:55:00 UTC
Updated	2021-11-10 15:54:00 UTC
Description	Heap-based buffer overflow in compression-pointer processing in core/ngx_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	lists.opensuse.org	Mailing List, Third Party A

Changeset 4268:25ddf6afc0ff – nginx	CONFIRM	trac.nginx.org	Issue Tracking, Patch, V
oss-security - Re: CVE Request: nginx resolver heap overflow	MLIST	openwall.com	Mailing List, Patch, Third
www.nginx.org/en/CHANGES-1.0	CONFIRM	www.nginx.org	Release Notes, Vendor A
[SECURITY] Fedora 16 Update: nginx-1.0.10-1.fc16	FEDORA	lists.fedoraproject.org	Third Party Advisory
nginx DNS Resolver Remote Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VD
About Secunia Research | Flexera	SECUNIA	secunia.com	Third Party Advisory
Gentoo Linux Documentation -- nginx: Multiple vulnerabilities	GENTOO	security.gentoo.org	Third Party Advisory
Security Alerts - Secunia	SECUNIA	secunia.com	Third Party Advisory
oss-security - CVE Request: nginx resolver heap overflow	MLIST	openwall.com	Mailing List, Patch, Third
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.

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