



# CVE-2011-0411

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

## Summary

<b>CVE</b>	CVE-2011-0411
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-03-16 22:55:00 UTC
<b>Updated</b>	2021-08-10 12:15:00 UTC
<b>Description</b>	The STARTTLS implementation in Postfix 2.4.x before 2.4.16, 2.5.x before 2.5.12, 2.6.x before 2.6.9, and 2.7.x before 2.7.5

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postfix	Postfix	2.4	All	All	All
Application	Postfix	Postfix	2.4.0	All	All	All
Application	Postfix	Postfix	2.4.1	All	All	All
Application	Postfix	Postfix	2.4.10	All	All	All
Application	Postfix	Postfix	2.4.11	All	All	All
Application	Postfix	Postfix	2.4.12	All	All	All
Application	Postfix	Postfix	2.4.13	All	All	All
Application	Postfix	Postfix	2.4.14	All	All	All
Application	Postfix	Postfix	2.4.15	All	All	All
Application	Postfix	Postfix	2.4.2	All	All	All
Application	Postfix	Postfix	2.4.3	All	All	All
Application	Postfix	Postfix	2.4.4	All	All	All
Application	Postfix	Postfix	2.4.5	All	All	All
Application	Postfix	Postfix	2.4.6	All	All	All
Application	Postfix	Postfix	2.4.7	All	All	All
Application	Postfix	Postfix	2.4.8	All	All	All
Application	Postfix	Postfix	2.4.9	All	All	All

Application	Postfix	Postfix	2.5.0	All	All	All
Application	Postfix	Postfix	2.5.1	All	All	All
Application	Postfix	Postfix	2.5.10	All	All	All
Application	Postfix	Postfix	2.5.11	All	All	All
Application	Postfix	Postfix	2.5.2	All	All	All
Application	Postfix	Postfix	2.5.3	All	All	All
Application	Postfix	Postfix	2.5.4	All	All	All
Application	Postfix	Postfix	2.5.5	All	All	All
Application	Postfix	Postfix	2.5.6	All	All	All
Application	Postfix	Postfix	2.5.7	All	All	All
Application	Postfix	Postfix	2.5.8	All	All	All
Application	Postfix	Postfix	2.5.9	All	All	All
Application	Postfix	Postfix	2.6	All	All	All
Application	Postfix	Postfix	2.6.0	All	All	All
Application	Postfix	Postfix	2.6.1	All	All	All
Application	Postfix	Postfix	2.6.2	All	All	All
Application	Postfix	Postfix	2.6.3	All	All	All
Application	Postfix	Postfix	2.6.4	All	All	All
Application	Postfix	Postfix	2.6.5	All	All	All
Application	Postfix	Postfix	2.6.6	All	All	All
Application	Postfix	Postfix	2.6.7	All	All	All
Application	Postfix	Postfix	2.6.8	All	All	All
Application	Postfix	Postfix	2.7.0	All	All	All
Application	Postfix	Postfix	2.7.1	All	All	All
Application	Postfix	Postfix	2.7.2	All	All	All
Application	Postfix	Postfix	2.4	All	All	All
Application	Postfix	Postfix	2.4.0	All	All	All
Application	Postfix	Postfix	2.4.1	All	All	All
Application	Postfix	Postfix	2.4.10	All	All	All
Application	Postfix	Postfix	2.4.11	All	All	All
Application	Postfix	Postfix	2.4.12	All	All	All
Application	Postfix	Postfix	2.4.13	All	All	All
Application	Postfix	Postfix	2.4.14	All	All	All
Application	Postfix	Postfix	2.4.15	All	All	All
Application	Postfix	Postfix	2.4.2	All	All	All

Application	Postfix	Postfix	2.4.3	All	All	All
Application	Postfix	Postfix	2.4.4	All	All	All
Application	Postfix	Postfix	2.4.5	All	All	All
Application	Postfix	Postfix	2.4.6	All	All	All
Application	Postfix	Postfix	2.4.7	All	All	All
Application	Postfix	Postfix	2.4.8	All	All	All
Application	Postfix	Postfix	2.4.9	All	All	All
Application	Postfix	Postfix	2.5.0	All	All	All
Application	Postfix	Postfix	2.5.1	All	All	All
Application	Postfix	Postfix	2.5.10	All	All	All
Application	Postfix	Postfix	2.5.11	All	All	All
Application	Postfix	Postfix	2.5.2	All	All	All
Application	Postfix	Postfix	2.5.3	All	All	All
Application	Postfix	Postfix	2.5.4	All	All	All
Application	Postfix	Postfix	2.5.5	All	All	All
Application	Postfix	Postfix	2.5.6	All	All	All
Application	Postfix	Postfix	2.5.7	All	All	All
Application	Postfix	Postfix	2.5.8	All	All	All
Application	Postfix	Postfix	2.5.9	All	All	All
Application	Postfix	Postfix	2.6	All	All	All
Application	Postfix	Postfix	2.6.0	All	All	All
Application	Postfix	Postfix	2.6.1	All	All	All
Application	Postfix	Postfix	2.6.2	All	All	All
Application	Postfix	Postfix	2.6.3	All	All	All
Application	Postfix	Postfix	2.6.4	All	All	All
Application	Postfix	Postfix	2.6.5	All	All	All
Application	Postfix	Postfix	2.6.6	All	All	All
Application	Postfix	Postfix	2.6.7	All	All	All
Application	Postfix	Postfix	2.6.8	All	All	All
Application	Postfix	Postfix	2.7.0	All	All	All
Application	Postfix	Postfix	2.7.1	All	All	All
Application	Postfix	Postfix	2.7.2	All	All	All

## References

Reference	Source	Link
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:009	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Plaintext command injection in multiple implementations of STARTTLS (CVE-2011-0411)	CONFIRM	<a href="http://www.postfix.org">www.postfix.org</a>
Postfix Plaintext to TLS Switching Error Lets Remote Users Inject Plaintext Commands - SecurityTracker	SECTRACK	<a href="http://securitytracker.com">securitytracker.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Gentoo Linux Documentation -- Postfix: Multiple vulnerabilities	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
Postfix "STARTTLS" Plaintext Injection Vulnerability - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
71021	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>
oss-security - STARTTLS vulnerabilities	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
cpuapr2011	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>
Debian -- Security Information -- DSA-2233-1 postfix	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
APPLE-SA-2011-10-12-3 OS X Lion v10.7.2 and Security Update 2011-006	APPLE	<a href="http://lists.apple.com">lists.apple.com</a>
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Fedora update for postfix - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
About the security content of OS X Lion v10.7.2 and Security Update 2011-006	CONFIRM	<a href="http://support.apple.com">support.apple.com</a>
Postfix Information for VU#555316	CONFIRM	<a href="http://www.kb.cert.org">www.kb.cert.org</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
US-CERT Vulnerability Note VU#555316 - STARTTLS plaintext command injection vulnerability	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>
Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	CONFIRM	<a href="http://kb.juniper.net">kb.juniper.net</a>
[SECURITY] Fedora 13 Update: postfix-2.7.3-1.fc13	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 14 Update: postfix-2.7.3-1.fc14	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web](http://www.mitre.org)

[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)**