CVE-2011-0411

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2011-0411
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-16 22:55:00 UTC
Updated	2021-08-10 12:15:00 UTC
Description	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 2.7.3

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	lists.opensuse.org

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

No vendor comments have been submitted for this CVE.

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

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report