

localhost 11/24/14:23.00 system check

Date: Mon, 24 Nov 2014 23:00:02 -0600
To: cpollock@embarqmail.com
From: root <cpollock@embarqmail.com>

Security Violations

==--==
Nov 24 22:00:04 localhost postfix/smtp[27898]: C722D1000A1D: to=
<cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,
delay=1.7, delays=0.51/0.26/0.22/0.69, dsn=2.0.0, status=sent (250 SPF
validation soft failure)

Unusual System Events

==--==
Nov 24 22:00:02 localhost postfix/pickup[7495]: C722D1000A1D: uid=0 from=
<root>
Nov 24 22:00:02 localhost postfix/cleanup[27896]: C722D1000A1D: message-id=
<20141125040002.C722D1000A1D@cpollock.localdomain>
Nov 24 22:00:03 localhost postfix/qmgr[2667]: C722D1000A1D: from=
<cpollock@embarqmail.com>, size=19001, nrcpt=1 (queue active)
Nov 24 22:00:04 localhost postfix/smtp[27898]: C722D1000A1D: to=
<cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,
delay=1.7, delays=0.51/0.26/0.22/0.69, dsn=2.0.0, status=sent (250 SPF
validation soft failure)
Nov 24 22:00:04 localhost postfix/qmgr[2667]: C722D1000A1D: removed
Nov 24 22:00:26 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17042, sent=1437332, time=96
Nov 24 22:00:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:00:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57373], protocol=IMAP
Nov 24 22:02:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17042, sent=1437332, time=92
Nov 24 22:02:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:02:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57415], protocol=IMAP
Nov 24 22:02:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:02:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57416], protocol=IMAP
Nov 24 22:04:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=133, sent=19689, time=90
Nov 24 22:04:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=2227, body=0, rcvd=16998, sent=1420323, time=90
Nov 24 22:04:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:04:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57425], protocol=IMAP
Nov 24 22:06:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17042, sent=1437367, time=92
Nov 24 22:06:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:06:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57442], protocol=IMAP
Nov 24 22:08:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17042, sent=1437367, time=92
Nov 24 22:08:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:08:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57460], protocol=IMAP
Nov 24 22:08:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:08:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57461], protocol=IMAP
Nov 24 22:09:31 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53233 to port 783, fd 5
Nov 24 22:09:31 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:09:31 localhost spamd[1511]: spamd: processing message
<52B4453E4614AA721B8DD2FF9587C9F2-
8d9c28a5cf254971876dce9c302e6f08@response.foxnews.com> for chris:1000
Nov 24 22:06:58 localhost clamd[2290]: message repeated 2 times: [
SelfCheck: Database status OK.]
Nov 24 22:09:32 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 1614, fd 13
Nov 24 22:09:50 localhost spamd[1511]: spamd: clean message (-114.0/5.0) for
chris:1000 in 19.0 seconds, 5165 bytes.
Nov 24 22:09:50 localhost spamd[1511]: spamd: result: . -114 -
AWL,BAYES_00,DCC_CHECK,DCC_CHECK_NEGATIVE,DIGEST_MULTIPLE,DKIM_SIGNED,DKIM_VALID,DKIM_VALID_AU,HTML_IMAGE_ONLY_24,HTML_MESSAGE
scantime=19.0,size=5165,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr=::1,rport=53233,mid=<52B4453E4614AA721B8DD2FF9587C9F2-
8d9c28a5cf254971876dce9c302e6f08@response.foxnews.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:10:21 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=133, sent=19689, time=91
Nov 24 22:10:21 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=16946, sent=1417953, time=91
Nov 24 22:10:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:10:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57473], protocol=IMAP

```

port=[57470], protocol=IMAP
Nov 24 22:10:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:10:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57471], protocol=IMAP
Nov 24 22:12:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=7218, body=0, rcvd=17061, sent=1438871, time=90
Nov 24 22:12:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=133, sent=19689, time=90
Nov 24 22:12:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:12:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57475], protocol=IMAP
Nov 24 22:14:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17038, sent=1450728, time=92
Nov 24 22:14:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:14:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57478], protocol=IMAP
Nov 24 22:14:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:14:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57479], protocol=IMAP
Nov 24 22:16:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=16942, sent=1431314, time=90
Nov 24 22:16:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=133, sent=19689, time=90
Nov 24 22:16:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:16:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57486], protocol=IMAP
Nov 24 22:16:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:16:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57487], protocol=IMAP
Nov 24 22:17:56 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53261 to port 783, fd 5
Nov 24 22:17:56 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:17:56 localhost spamd[1511]: spamd: processing message
<547401D1.4020108@canonical.com> for chris:1000
Nov 24 22:17:56 localhost clamd[2290]: SelfCheck: Database status OK.
Nov 24 22:17:56 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 1038, fd 13
Nov 24 22:18:10 localhost spamd[1511]: spamd: clean message (-0.3/5.0) for
chris:1000 in 14.6 seconds, 7697 bytes.
Nov 24 22:18:10 localhost spamd[1511]: spamd: result: . 0 -
AWL,BAYES_00,HEADER_FROM_DIFFERENT_DOMAINS,RCVD_IN_MSPIKE_H4,RCVD_IN_MSPIKE_WL,RDNS_NONE,UNPARSEABLE_RELAY
scantime=14.6,size=7697,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr>:::1,rport=53261,mid=
<547401D1.4020108@canonical.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:18:11 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53267 to port 783, fd 5
Nov 24 22:18:11 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:18:11 localhost spamd[1511]: spamd: processing message
<547401B0.4030808@canonical.com> for chris:1000
Nov 24 22:18:11 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 1463, fd 13
Nov 24 22:18:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=16942, sent=1431314, time=90
Nov 24 22:18:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=133, sent=19689, time=90
Nov 24 22:18:24 localhost spamd[1511]: spamd: clean message (-0.3/5.0) for
chris:1000 in 13.1 seconds, 8083 bytes.
Nov 24 22:18:24 localhost spamd[1511]: spamd: result: . 0 -
AWL,BAYES_00,HEADER_FROM_DIFFERENT_DOMAINS,RCVD_IN_MSPIKE_H4,RCVD_IN_MSPIKE_WL,RDNS_NONE,UNPARSEABLE_RELAY
scantime=13.1,size=8083,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr>:::1,rport=53267,mid=
<547401B0.4030808@canonical.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:18:24 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53270 to port 783, fd 5
Nov 24 22:18:24 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:18:24 localhost spamd[1511]: spamd: processing message
<547401F1.4070900@canonical.com> for chris:1000
Nov 24 22:18:24 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 1606, fd 13
Nov 24 22:18:37 localhost spamd[1511]: spamd: clean message (-0.3/5.0) for
chris:1000 in 12.7 seconds, 10812 bytes.
Nov 24 22:18:37 localhost spamd[1511]: spamd: result: . 0 -
AWL,BAYES_00,HEADER_FROM_DIFFERENT_DOMAINS,RCVD_IN_MSPIKE_H4,RCVD_IN_MSPIKE_WL,RDNS_NONE,UNPARSEABLE_RELAY
scantime=12.7,size=10812,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr>:::1,rport=53270,mid=
<547401F1.4070900@canonical.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:18:37 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53273 to port 783, fd 5
Nov 24 22:18:37 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:18:37 localhost spamd[1511]: spamd: processing message
<54740210.7020509@canonical.com> for chris:1000
Nov 24 22:18:37 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 1820, fd 13
Nov 24 22:18:50 localhost spamd[1511]: spamd: clean message (-0.4/5.0) for
chris:1000 in 12.9 seconds, 10569 bytes.
Nov 24 22:18:50 localhost spamd[1511]: spamd: result: . 0 -
AWL,BAYES_00,HEADER_FROM_DIFFERENT_DOMAINS,RCVD_IN_MSPIKE_H4,RCVD_IN_MSPIKE_WL,RDNS_NONE,UNPARSEABLE_RELAY

```

```

time=12.9,size=10569,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr:::1,rport=53273,mid=
<54740210.7020509@canonical.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:18:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:18:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57507], protocol=IMAP
Nov 24 22:20:50 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53281 to port 783, fd 5
Nov 24 22:20:50 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:20:50 localhost spamd[1511]: spamd: processing message
<5474022F.4060400@canonical.com> for chris:1000
Nov 24 22:20:50 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 1935, fd 13
Nov 24 22:21:03 localhost spamd[1511]: spamd: clean message (-0.4/5.0) for
chris:1000 in 12.6 seconds, 8390 bytes.
Nov 24 22:21:03 localhost spamd[1511]: spamd: result: . 0 -
AWL,BAYES_00,HEADER_FROM_DIFFERENT_DOMAINS,RCVD_IN_MSPIKE_H4,RCVD_IN_MSPIKE_WL,RDNS_NONE,UNPARSEABLE_RELAY
scantime=12.6,size=8390,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr:::1,rport=53281,mid=
<5474022F.4060400@canonical.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:21:03 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53285 to port 783, fd 5
Nov 24 22:21:03 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:21:03 localhost spamd[1511]: spamd: processing message
<5474024F.3040400@canonical.com> for chris:1000
Nov 24 22:21:03 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 1372, fd 13
Nov 24 22:21:15 localhost spamd[1511]: spamd: clean message (-0.4/5.0) for
chris:1000 in 12.5 seconds, 8590 bytes.
Nov 24 22:21:15 localhost spamd[1511]: spamd: result: . 0 -
AWL,BAYES_00,HEADER_FROM_DIFFERENT_DOMAINS,RCVD_IN_MSPIKE_H4,RCVD_IN_MSPIKE_WL,RDNS_NONE,UNPARSEABLE_RELAY
scantime=12.5,size=8590,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr:::1,rport=53285,mid=
<5474024F.3040400@canonical.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:21:16 localhost spamd[1511]: spamd: connection from ip6-localhost
[::1]:53288 to port 783, fd 5
Nov 24 22:21:16 localhost spamd[1511]: spamd: setuid to chris succeeded
Nov 24 22:21:16 localhost spamd[1511]: spamd: processing message
<54740282.30501@canonical.com> for chris:1000
Nov 24 22:21:16 localhost clamd[2290]: Accepted connection from 127.0.0.1 on
port 2017, fd 13
Nov 24 22:21:26 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:21:26 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57520], protocol=IMAP
Nov 24 22:21:28 localhost spamd[1511]: spamd: clean message (-0.4/5.0) for
chris:1000 in 12.4 seconds, 8298 bytes.
Nov 24 22:21:28 localhost spamd[1511]: spamd: result: . 0 -
AWL,BAYES_00,HEADER_FROM_DIFFERENT_DOMAINS,RCVD_IN_MSPIKE_H4,RCVD_IN_MSPIKE_WL,RDNS_NONE,UNPARSEABLE_RELAY
scantime=12.4,size=8298,user=chris,uid=1000,required_score=5.0,rhost=ip6-
localhost,raddr:::1,rport=53288,mid=
<54740282.30501@canonical.com>,bayes=0.000000,autolearn=disabled
Nov 24 22:22:56 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=35378, body=67137, rcvd=46599, sent=3023803,
time=246
Nov 24 22:22:56 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=26562, body=72541, rcvd=17660, sent=1566999,
time=90
Nov 24 22:24:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:24:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57556], protocol=IMAP
Nov 24 22:26:23 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17106, sent=1451101, time=93
Nov 24 22:26:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:26:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57589], protocol=IMAP
Nov 24 22:28:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17060, sent=1451073, time=92
Nov 24 22:28:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:28:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57606], protocol=IMAP
Nov 24 22:30:25 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17060, sent=1451073, time=95
Nov 24 22:30:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:30:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57611], protocol=IMAP
Nov 24 22:31:16 localhost clamd[2290]: SelfCheck: Database status OK.
Nov 24 22:32:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17060, sent=1451073, time=92
Nov 24 22:32:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:32:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57613], protocol=IMAP
Nov 24 22:34:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17060, sent=1451073, time=92
Nov 24 22:34:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:34:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57666], protocol=IMAP

```

```
Nov 24 22:36:00 localhost dbus[381]: [system] Activating service
name='org.freedesktop.hostname1' (using servicehelper)
Nov 24 22:36:01 localhost dbus[381]: [system] Successfully activated service
'org.freedesktop.hostname1'
Nov 24 22:36:01 localhost kernel: [12276.249320] systemd-hostnamed[29473]:
Warning: nss-myhostname is not installed. Changing the local hostname might
make it unresolveable. Please install nss-myhostname!
Nov 24 22:36:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17060, sent=1451073, time=92
Nov 24 22:36:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:36:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57670], protocol=IMAP
Nov 24 22:36:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:36:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57671], protocol=IMAP
Nov 24 22:38:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=133, sent=19689, time=90
Nov 24 22:38:20 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=16964, sent=1431659, time=90
Nov 24 22:38:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:38:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57686], protocol=IMAP
Nov 24 22:40:25 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17060, sent=1451073, time=95
Nov 24 22:40:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:40:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57749], protocol=IMAP
Nov 24 22:42:22 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=0, rcvd=17060, sent=1451073, time=92
Nov 24 22:42:50 localhost imapd: Connection, ip=[::ffff:127.0.0.1]
Nov 24 22:42:50 localhost imapd: LOGIN, user=chris, ip=[::ffff:127.0.0.1],
port=[57836], protocol=IMAP
Nov 24 22:43:12 localhost imapd: DISCONNECTED, user=chris, ip=
[::ffff:127.0.0.1], headers=0, body=9293, rcvd=17165, sent=1460871, time=22
Nov 24 22:43:23 localhost kernel: [12718.904386] usb 2-2: USB disconnect,
device number 2
Nov 24 22:43:24 localhost colord: device removed: sysfs-(null)
Nov 24 22:43:24 localhost colord: device removed: sysfs-SAMSUNG-
SAMSUNG_Android
```