

# [UNIX] Posfix Remote DoS / Postfix Bounce Scanning

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0009.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 08/05/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 5 Aug 2003 11:03:50 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

-----  
Posfix Remote DoS / Postfix Bounce Scanning  
-----

## SUMMARY

<<http://postfix.org>> Postfix is "Wietse Venema's mailer that started life as an alternative to the widely-used Sendmail program. Postfix attempts to be fast, easy to administer, and secure, while at the same time being Sendmail compatible enough to not upset existing users. Thus, the outside has a sendmail-ish flavor, but the inside is completely different".

Two vulnerabilities discovered in Postfix, allow a remote user to DoS Postfix, and to maliciously use Postfix as a DDoS agent or for probing networks.

## DETAILS

Vulnerable Systems:

\* Postfix versions up to and including 1.1.12

## Securiteam: [UNIX] Posfix Remote DoS / Postfix Bounce Scanning

Immune Systems:

- \* Postfix version 2.0 and up
- \* Postfix version 1.1.13

Postfix 1.1.12 remote DoS:

There is a remotely exploitable denial of service vulnerability in Postfix up to and including 1.1.12. The vulnerability does not affect the most current version, 2.0, due to a major overhaul of the address parsing code. Releases prior to 1.1.9 are not vulnerable by default, but will be exposed if `append_dot_mydomain` is turned off in the configuration file (see section 3 for more details).

Recent 1.1 releases, having no publicly disclosed security problems, are still commonly used and shipped in several popular Linux distributions, including Red Hat 9 or Debian 3.0 (woody) – those distributions both ship 1.1.11.

The vulnerability lies in the address parser code. By supplying a remote SMTP listener with a malformed envelope address, it is possible to, depending on the method, either:

- Cause the queue manager, `nqmgr`, to lock up permanently, effectively stopping any queue processing – all mail traffic suppressed. Restarting the service has no effect – a specific entry has to be removed from the queue to fix the problem. For that reason, a built-in watchdog that restarts `nqmgr` after a period of non responsive behavior, is not able to cause a recovery from this condition.

The attack can be performed by forcing the service to queue a mail to an address that would generate a bounce – depending on the configuration, it can be `<nonexistent@local-server-name>`, or, if user names are being checked, `<nonexistent@[127.0.0.1]>`. The "mail from" or "Errors-To" address should be set to `<.!>` or `<.!@local-server-name>`. An attempt to parse and rewrite the latter address when preparing a bounce will lock up the service.

..Or...

- Lock up a single instance of the SMTP listener in a unusable state that persists after the client disconnects. By repeating this, it is possible to DoS the service (or entire system, depending on the configuration) in a very effective manner.

This can be achieved by providing any valid "MAIL FROM" in a SMTP conversation, and then supplying a "RCPT TO" similar to "MAIL FROM" in the previous example. If the server is vulnerable, the session should freeze at this point.

The latter approach, since it only creates a single stalled process, is a less intrusive method of testing your systems for this issue remotely.

## Securiteam: [UNIX] Posfix Remote DoS / Postfix Bounce Scanning

The attack can be detected by looking for "resolve\_clnt\_query: NULL recipient" in your maillog. It is then necessary to find the problematic entry in the queue and remove it manually, then restart the service.

It should be noted that it is often possible to attack instances that do not have port 25 reachable from the Internet – envelope addresses and certain headers such as Errors-To may very well be preserved when a message is relayed via another system or service.

Postfix 1.1.11 Bounce scan / DDoS agent issue:

There is a remotely exploitable vulnerability in Postfix 1.1.11 (and earlier versions). Postfix 1.1.12 and 2.0 is NOT affected. The problem was apparently spotted and fixed in 1.1.12 (note 200221121 in HISTORY file), although it has been tagged as a change preventing bogus log entries, and not described as a security issue; there was no public information or discussion about its implications on security forums, not prompting users to upgrade. It might be that the significance of this problem was simply overlooked.

Since the issue has been rediscovered during the analysis of the previous issue, Michal decided it is worth mentioning here, especially since 1.1.11 is shipped all over the place.

The problem enables an attacker to use Postfix 1.1.11 as a DDoS agent or for bounce scans of other hosts on the Internet, or probing Firewalled internal networks. The problem is triggered by an attempt to deliver to:  
<[server\_ip]:service!@local-host-name>

This address will cause Postfix to connect an arbitrary IP at an arbitrary port and attempt to talk SMTP. The conversation will likely fail before any user-dependent data is sent to the remote party, which limits the exposure, but is sufficient to bounce-scan.

The address can be either sent in "RCPT TO" (the attacker would have the right to relay to this system, which makes it a viable method of bounce scanning your ISP/mail account provider). In which case the sender would then look for bounces stating the problem (SMTP conversation error, connection timeout or connection refused), or in "MAIL FROM" / Errors-To, in which case, the attacker can likely perform a queue timing attack to detect whether a port is open by inserting control messages that are intended to bounce.

When a port is open, SMTP greeting timeout occurs after a longer while, pausing queue processing. When a port is closed, the entry is immediately marked as deferred and queue processing continues.

It is also possible to use this problem to stage a DDoS attack, by making a number of Postfix hosts around the world attempt to connect services on a particular machine repeatedly, until each queue entry finally expires and is discarded or delivered to postmaster.

## Securiteam: [UNIX] Posfix Remote DoS / Postfix Bounce Scanning

### Vendor Status:

To find out your Postfix version, use the command "postconf mail\_version". Versions prior to 1.1 show a date instead of a version number (e.g., Postfix-20010228-pl08). Versions 1.1 and later may show a date in addition to the version number (e.g., 2.0.14-20030717).

### Postfix versions 2.0 and later:

Not vulnerable, because the trivial-rewrite code was completely restructured. The current Postfix version is 2.0.13.

A not vulnerable Postfix version can protect vulnerable Postfix systems as described in the workarounds section below.

### Postfix versions 1.1.9 up to 1.1.12:

These are vulnerable, and are fixed by upgrading to version 1.1.13 which will be made available via <http://www.postfix.org/> and via individual vendors, or by applying the patch below. The workarounds section below has instructions for sites that cannot upgrade Postfix immediately.

### Postfix versions prior to 1.1.9:

These become vulnerable only when the append\_dot\_mydomain feature is set to "no" (you can verify this with the command "postconf append\_dot\_mydomain"). Use the command "postconf -e append\_dot\_mydomain=yes" to update the setting if necessary.

Sites that must use "append\_dot\_mydomain=no" should either upgrade to a fixed Postfix version, or should apply the one-line patch at the end of this text. This patch has been tested with Postfix versions back to 19991231.

### Workarounds for Postfix versions 1.1.9 up to 1.1.12:

Verify that the append\_dot\_mydomain feature is set to "yes" by using the command "postconf append\_dot\_mydomain". Use the command "postconf -e append\_dot\_mydomain=yes" to update the setting if necessary.

Sites that must use "append\_dot\_mydomain=no" should either upgrade to a fixed Postfix version, or should apply the one-line patch at the end of this text.

Specify "resolve\_dequoted\_address=no" in main.cf.

An additional workaround is needed for hosts that must forward mail from the Internet to, for example, primary MX hosts or to internal hosts. This is because with resolve\_dequoted\_address=no, Postfix no longer recognizes user@bad.domainn@good.domain as a mail relaying attempt. To close this loophole, use a regular expression to block sender-specified routing in SMTP recipient addresses:

```
/etc/postfix/main.cf:  
smtpd_recipient_restrictions =  
    permit_mynetworks,
```

## Securiteam: [UNIX] Posfix Remote DoS / Postfix Bounce Scanning

```
check_recipient_access
regexp:/etc/postfix/recipient_regexp
...other restrictions...
check_relay_domains
```

```
/etc/postfix/recipient_regexp:
/[%!@].*[%!@]/ 550 Sender-specified routing rejected
```

Workarounds to protect vulnerable down-stream Postfix systems:  
Reject Errors-To: message headers with multiple routing operators:

```
/etc/postfix/main.cf:
header_checks = regexp:/etc/postfix/header_checks
```

```
/etc/postfix/header_checks:
/^errors-to:.*[%!@].*[%!@]/ reject
```

Reject SMTP sender addresses with multiple routing operators:

```
/etc/postfix/main.cf:
smtpd_sender_restrictions =
check_sender_access regexp:/etc/postfix/sender_regexp
...other restrictions...
```

```
/etc/postfix/sender_regexp:
/[%!@].*[%!@]/ 550 Sender-specified routing rejected
```

```
diff -cr /tmp/postfix-1.1.12/src/trivial-rewrite/resolve.c
src/trivial-rewrite/resolve.c
*** /tmp/postfix-1.1.12/src/trivial-rewrite/resolve.c Fri Nov 22 12:32:33
2002
---- src/trivial-rewrite/resolve.c Mon Jul 28 11:36:49 2003
*****
*** 148,153 ****
---- 148,154 ----
    if (saved_domain)
        tok822_free_tree(saved_domain);
        saved_domain = domain;
+ domain = 0;
    }

/*
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:lcantuf@ghettot.org>> Michal Zalewski

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

Securiteam: [UNIX] Posfix Remote DoS / Postfix Bounce Scanning

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.