

# [UNIX] Remote Vulnerability in Horde MTA

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0053.html>

---

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

**Date:** 08/18/03

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

Date: 18 Aug 2003 14:13:32 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Remote Vulnerability in Horde MTA

---

## SUMMARY

<<http://www.horde.org>> Horde is "both a piece of software and a project. The Horde Project comprises a set of Web-based productivity, messaging, and project-management applications, each of which is described below. The Horde Framework is a common code-base used by Horde applications, including libraries and a common user interface. The Horde Framework doesn't do anything on its own; as a user, you will always be interacting with a Horde-based application".

<<http://www.horde.org/imp/>> IMP is "the Internet Messaging Program (formerly, among other things, the IMAP web mail Program), a web mail system and a component of the Horde project. IMP is the most widely deployed component of Horde. IMP offers most of the features users have come to expect from their conventional mail programs, including attachments, spell-check, address books, multiple folders, and multiple-language support".

An attacker could send an email to the victim using Horde MTA and cause him to unwillingly reveal his Horde session id

## DETAILS

## Securiteam: [UNIX] Remote Vulnerability in Horde MTA

### Vulnerable Systems:

- \* Horde MTA versions prior to 2.2.4

### Immune Systems:

- \* Horde MTA version 2.24

### Example:

<http://MYSITE.MYSOCIETY.NET/HORDE/IMP/MESSAGE.PHP?HORDE=FC235847D2C8A88190C879B290D12>

As you can see by above example, the session can be grabbed by very simple Referer monitoring, since the session becomes obsolete after approximately 20 minutes an attacker has a lot of time to hijack the Horde account.

### Vendor Status:

The vulnerability has been fixed in version 2.2.4, see:

<<http://lists.horde.org/archives/announce/2003/000051.html>>

<http://lists.horde.org/archives/announce/2003/000051.html>.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:puccio@pucciolab.org>>  
Vincenzo 'puccio' Ciaglia

=====

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)

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.