

# MDaemon SMTP/POP/IMAP server =>v.6.7.5: IMAP buffer overflow

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-04/0364.html>

---

**From:** D4rkGr3y (*grey\_1999\_at\_mail.ru*)  
**Date:** 04/27/03

Date: Sat, 26 Apr 2003 20:27:01 -0700  
To: bugtraq@securityfocus.com

-----BEGIN PGP SIGNED MESSAGE-----

```
#####*
# Damage Hacking Group security advisory
# www.dhgroup.org
#####*
#Product: MDAemon SMTP/POP/IMAP server =>v.6.7.5
#Authors: Alt-N Technologies [www.mdaemon.com]
#Vulnerability: remote buffer overflow in IMAP service
#####*
```

#Overview#-----#

-- From help-file:

"MDaemon Server v6 brings SMTP/POP/IMAP and MIME mail services commonplace on UNIX hosts and the Internet to Windows based servers and microcomputers. MDAemon is designed to manage the email needs of any number of individual users and comes complete with a powerful set of integrated tools for managing mail accounts and message formats.

MDaemon offers a scalable SMTP, POP3, and IMAP4 mail server complete with LDAP support, an integrated browser-based email client, content filtering, spam blockers, extensive security features, and more."

#Problem#-----#

Remote buffer overflow was found in MDAemon IMAP service.

A remote authorized user can execute arbitrary code on the server with SYSTEM privileges.

"Create" command for the IMAP server do not have proper bounds checking, enabling a user to shutdown the service remotely. It should be noted that a user account is required.

Remote authorized user may create new mailbox via IMAP service with mailbox name more then 1Kb. In result, SMTP/POP/IMAP/LDAP will crash, but WorldClient and WebAdmin will work normally.

For example:

```
0 CREATE AAAAAAA..[1kb]..AAA
```

## SecurityFocus Bugtraq: MDaemon SMTP/POP/IMAP server =>v.6.7.5: IMAP buffer overflow

When we send "0 CREATE AAAAAAA..[1kb]..AAA", Server creates mailbox with name "AAAAA.. [202b..] AAA " and crash. Second time we exact also we can not attack, because the server will consider, that the mailbox "AAAAA...AAA" is already created and will refuse to process command. To bypass it, we must change any character from the first 202 characters (for example, create "BAAAAAA... AA" or "BBBBBBB...BB" instead of "AAAAA... AA").

A vulnerability may use to execute arbitrary code (the remote user can cause the EAX and EDI registers to be overwritten with arbitrary data). All code will be run with system privileges (if MDaemo