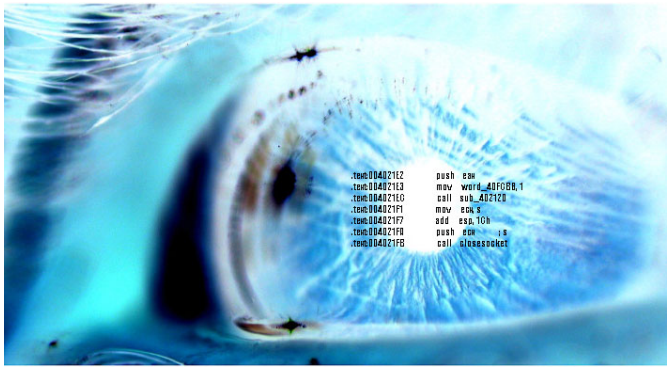
CIRT

Danish Computer Incident Response Team

Security advisory

MacAllan Mail Solution 4.0.6.8 (Build 786) multiple vulnerabilities



Discovered by Dennis Rand
advisory@cirt.dk
http://www.cirt.dk

Table of contents

Introduction

Problem

The Macallan mail solution 4.0.6.8 (Build 786) contains several vulnerabilities

- "Macallan Mail Solution Web Interface Authentication Bypass" similar to vulnerability reported earlier by Secunia http://secunia.com/advisories/10861/

- Denial of Service when requesting an overly long URL starting with an interrogation mark on the web server

What is Macallan Mail Solutions

Macallan Mail Solution is a Mail Server (SMTP/POP3/IMAP/HTTP) for Microsoft Windows XP™ and Microsoft Windows 2000™ that works with clients such as Microsoft Outlook Express™ or Microsoft Outlook™. Filtering mechanisms against Spammers using DNSBL (DNS Black List) and your own Keywords Black List / Friend List are included. Mechanisms against Virus can be used with your Anti-Virus. Replies can be sent automatically for those abusing Spam and Virus to providers.

http://perso.club-internet.fr/macallan/MMS/index.html

Timeline of public disclosure

- 04-12-2004 Vulnerability discovered
- 04-12-2004 Vendor contacted
  - macallan@club-internet.fr
- 31-12-2004 Public Disclosure

Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK
Questions regarding this issue should be directed to:

Dennis Rand
advisory@cirt.dk

Problem

Web Interface Authentication Bypass

First some look back in history, on the 2. December 2004 Secunia reported a similar problem:
It is possible to bypass the authentication in the web interface by sending a HTTP GET request with two slashes ("//") before the requested resource.

This issue was reported as a low risk vulnerability since it was according to the vendor, not possible to perform any administrative actions.

This problem has been fixed in the current version, BUT if a url-encoded "/" is used, it is still possible to gain access to the administrative interface and it is possible to relay messages through the web interface.
Another more easy way to bypass login is to just request a directory not existing and then the file you want to see.

Requesting long URL starting with an interrogation mark Denial of Service

When requesting a long URL starting with an interrogation mark, the web server will crash, and result in partial manipulation of the EIP.
The partial overwriting of the EIP does not seem to be exploitable, into where an attacker can run arbitrary code.

Technical details

Web Interface Authentication Bypass

When url-encoding a "/" into "%2f" or just requesting a none existing directory it is possible to bypass the logon authentication of the web server.
e.g.:

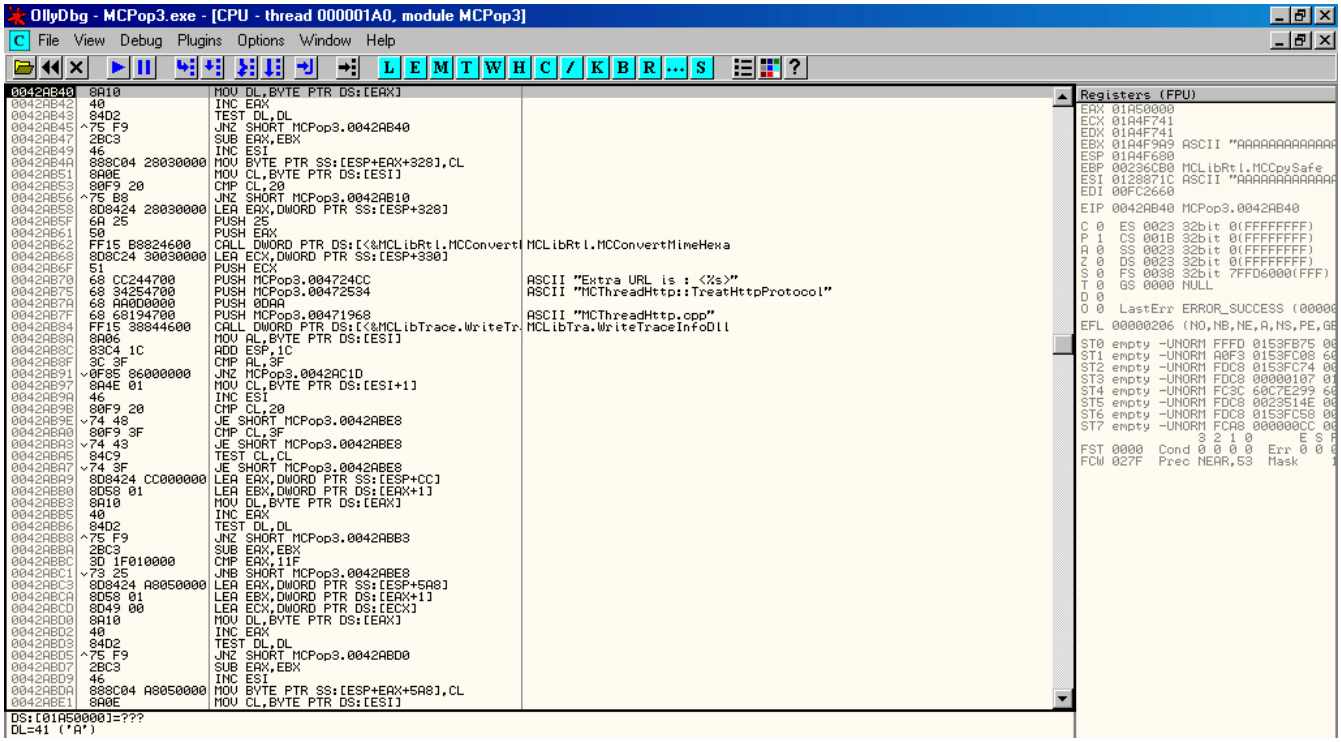
http://<Target>:8080/%2f/newmessage.html	→ Possible to relay messages
http://<Target>:8080/%2f/admin.html	→ Access to administrative interface
http://<Target>:8080/%2f/settings.html	→ Possible to change password

Or the maybe more easy way:

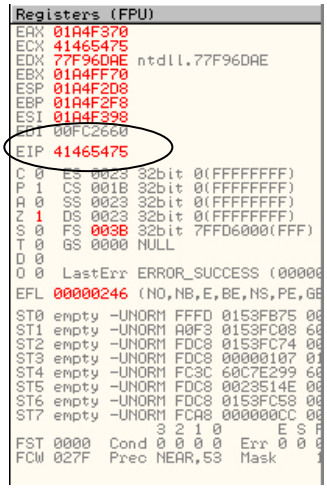
http://<Target>:8080/qwe/newmessage.html	→ Possible to relay messages
http://<Target>:8080/qwe/admin.html	→ Access to administrative interface
http://<Target>:8080/qwe/settings.html	→ Possible to change password

Requesting long URL starting with an interrogation mark Denial of Service

When requesting a "**GET /?<long request> HTTP/1.0**" the server will crash the MCPOP3 service running the web server and the POP3 daemon.



Figur 1 - Right after the attack has been made



Figur 2 - Here is the part where the EIP has been modified

It is here shown that the first part of the EIP has been overwritten by "**41**" that is the hex value of "**A**"

Corrective actions

Upgrade to version 4.1.1.0 or later, here the problem have been fixed.

Disclaimer