CSIS Advisory

Outlook Email File Attachment Denial of Service Vulnerability

Document written and evaluated by:
Sarid Harper
sha@csis.dk

Technical report

Publish date: november 26, 2010

Contents

1 Summary

A vulnerability has been discovered in Outlook, which can be exploited by malicious, anonymous individuals to cause a DoS (Denial of Service).

The vulnerability is caused as a result of the improper handling of email file attachments with no extension. This can be exploited to cause a DoS by tricking a user into clicking on an attachment with no file extension in the reading pane.

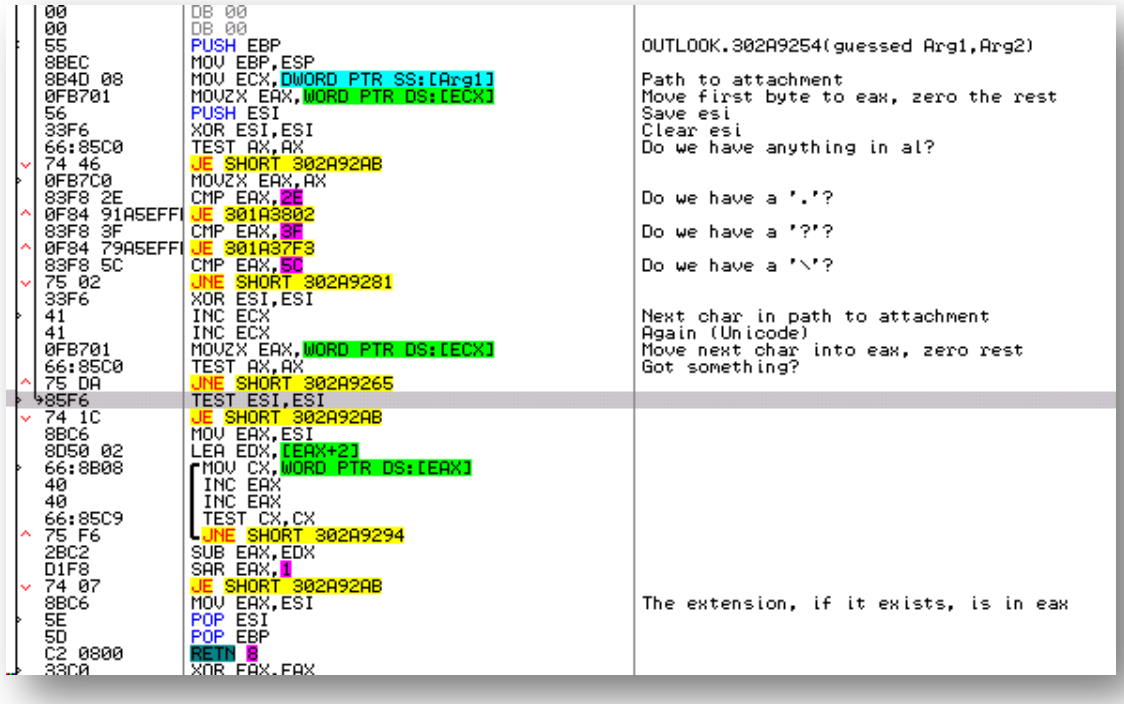
2 Affected Versions

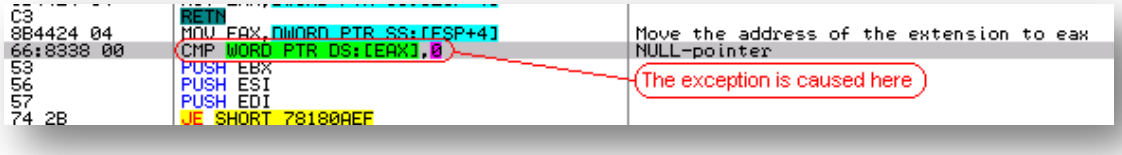
This vulnerability is confirmed in the following version:

- Microsoft Outlook 2007 (12.0.6539.5000) SP2 MSO (12.0.6545.5004)

Other versions may also be affected.

3 Screen-dumps





4 Resolution

Turn off the reading pane.

5 Time-line

1. Vulnerability identified: 03.09.10
2. Vendor informed: 19.11.10
3. Vendor response: 24.11.10
4. Vendor fix: Currently unavailable

6 Credits

Vulnerability identified by Sarid Harper of the CSIS Security Group.

7 References

Turn the Reading Pane off or on:

http://office.microsoft.com/en-us/outlook-help/make-changes-to-the-reading-preview-pane-HA010118503.aspx?CTT=1#_Toc267389729