

[NT] Internet Explorer and Access Allows Macros to be Executed Automatically

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0075.html>

From: support@securiteam.com

Date: 02/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 13 Feb 2002 10:09:29 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Internet Explorer and Access Allows Macros to be Executed Automatically

SUMMARY

GFI, developer of email content checking & network security software, has recently discovered a security flaw within Internet Explorer which allows a malicious user to run arbitrary code on a target machine as it attempts to view a website or an HTML email.

The problem is exploited by embedding a VBA code within an Access database file (.mdb) within an Outlook Express email file or Multipart HTML (mht) file.

If the email file is accessed using Internet Explorer, the attachment may be automatically executed without triggering any security alerts. The exploit will work regardless of the security level (GFI has also tested it with High Security and Restricted Zone).

This may be exploited through email by using an iframe tag or using Active Scripting to call the malicious file through an HTML email, allowing Internet Explorer to automatically access the exploit EML file.

DETAILS

Securiteam: [NT] Internet Explorer and Access Allows Macros to be Executed Automatically

Vulnerable systems:

- * Microsoft Access
- and
- * Internet Explorer version 5 up until version 6. Older versions may be vulnerable as well.
- * Outlook Express 2000,
- * Outlook Express 98,
- * Outlook 2000,
- * Outlook 98
- * possibly other HTML and/or JavaScript enabled email clients.

Vendor status:

Microsoft has been informed and we have worked with them to release a patch.

Proof of concept exploit:

A live example of the named exploit is available on:

<<http://www.gfi.com/emailsecuritytest>>
<http://www.gfi.com/emailsecuritytest>

Solution:

Filtering HTML email for JavaScript and similarly scripting capabilities as well as checking for IFRAME will prevent the exploit to be run through email.

GFI Security Labs also recommends filtering out mdb files.

You might also want to consider blocking access to EML, MHTML and MHT files through HTTP and SMTP. It is also important to apply the patch distributed by Microsoft.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sandro@gfi.com>> Sandro Gauci.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.

Securiteam: [NT] Internet Explorer and Access Allows Macros to be Executed Automatically

- **Previous message:** support@securiteam.com: "[\[EXPL\] Format String Vulnerability in VXPrint Allows Gaining of Arbitrary Privileges](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)