

[NT] McAfee Security Center MCINSCTL.DLL ActiveX Control File Overwrite

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00066.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 21 Dec 2005 17:04:08 +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>

McAfee Security Center MCINSCTL.DLL ActiveX Control File Overwrite

SUMMARY

" <<http://us.mcafee.com/root/catalog.asp>> McAfee VirusScan detects, blocks, and removes viruses and Spyware, that may result in the loss of your irreplaceable documents, such as digital photos, family movies, and financial spreadsheets, identity theft and slower PC performance."

Remote exploitation of an access control vulnerability in McAfee Security Center allows attackers to create or overwrite locally stored files.

DETAILS

Vulnerable Systems:

* McAfee VirusScan mcinsctl.dll version 4.0.0.83

The vulnerability specifically exists due to a registered ActiveX control failing to restrict which domains may load the control for execution. MCINSCTL.DLL as included with McAfee Security Center exports an object for logging called MCINSTALL.McLog. The McLog object is designed to allow Security Center to log to a file through the StartLog and AddLog methods. McAfee fails to restrict the ActiveX control from being loaded in

[NT] McAfee Security Center MCINSCTL.DLL ActiveX Control File Overwrite

arbitrary domains. As such, attackers can create a specially crafted web page utilizing the McLog object to create arbitrary files. This attack can lead to arbitrary code execution by a remote attacker.

Successful exploitation of this vulnerability allow attackers to create or append to arbitrary files. An attacker can write to a startup folder to execute arbitrary code during the next reboot or logon session. A user will not be required to authorize the object instantiation since the object is within a signed ActiveX control. A typical exploitation scenario would require an attacker to convince a targeted user to visit a malicious website.

This vulnerability hints at a new class of vulnerabilities that occur due to developers not using the IObjectSafetySiteLock() API to restrict domains that can load a particular ActiveX control. Vendors who distributed third-party ActiveX controls should be sure to use the IObjectSafetySiteLock() API in their applications.

Vendor Status:

"McAfee previously released updates to SecurityCenter that resolve this issue. All active McAfee SecurityCenter users, by default, should have automatically received the update, and will now have the fix for this vulnerability already installed on their computers.

To manually check for updates, users can right-click the McAfee system tray icon (white M on red background) and select 'Updates'. In the resulting dialog box, they should click 'Check Now' to check the server for updates. The user will be walked through the update process or be notified that all software is up to date. If a user has not yet registered, a registration web page or the registration wizard will pop-up, guiding the user through the update process.

McAfee's key priority is the security of our customers. In the event that a vulnerability is found within any of McAfee's software, we have a strong process in place to work closely with the relevant security research group to ensure the rapid and effective development of a fix and communication plan."

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3657>>
CVE-2005-3657

Disclosure Timeline:

11/15/2005 – Initial vendor notification
11/16/2005 – Initial vendor response
12/20/2005 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

[NT] McAfee Security Center MCINSCTL.DLL ActiveX Control File Overwrite

<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs.

The original article can be found at:

<<http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=358>>

<http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=358>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.

-
- Prev by Date: [**\[NT\] Qualcomm WorldMail IMAP Server String Literal Processing Overflow**](#)
 - Next by Date: [**\[UNIX\] Blender Integer Overflow Vulnerability \(BlenLoader, get_bhead\)**](#)
 - Previous by thread: [**\[NT\] Qualcomm WorldMail IMAP Server String Literal Processing Overflow**](#)
 - Next by thread: [**\[UNIX\] Blender Integer Overflow Vulnerability \(BlenLoader, get_bhead\)**](#)
 - Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)