March 17, 2005

McAfee Security Bulletin

Overview

McAfee is announcing to its' customers who are operating on a previous version of the McAfee VirusScan Engine (version 4320) are susceptible to a buffer overrun when scanning LHa files.

- **No action is required if your environment is currently running the 4400 Scan Engine (issued November 2004) or the Virus Definition (DAT) version is 4436 (issued March 1, 2005) or higher**

McAfee strongly encourages all McAfee customers to read the following bulletin and, if necessary, implement the recommendations listed below as soon as possible.

The automatic downloading and installation of updates and upgrades as a default setting in VirusScan assures the delivery of the latest product version to our customers. We urge all customers to verify that they have installed and deployed the 4436 DAT [or higher] and/or the 4400 Scan Engine. If running an earlier .DAT and the previous version of the McAfee VirusScan engine (4320), McAfee recommends that an update is performed. As of the writing of this security bulletin, there are no known public cases of exploit code that exist.

Summary of Vulnerabilities

CAN-2005-0643 - McAfee Engine Buffer Overflow when scanning LHa files

A vulnerability announcement in May 2004 prompted McAfee to inspect our technology to determine the susceptibility to the potential exploit. This inspection determined that the 4320 version of the McAfee Scan Engine was susceptible to a buffer overflow when scanning LHa files. An alteration to the configuration of the Scan Engine issued with the 4357 DAT file (issued May 2004) was made to eliminate the vulnerability within the 4320 Scan Engine.

Products affected: *Scan Engine 4320* – any McAfee point products still using the 4320 engine and DAT version less than 4357.

CAN-2005-0644- Engine Buffer Overflow when scanning malformed LHa files

In February 2005, a variation of this vulnerability was reported to McAfee by ISS X-Force. It was found that the 4320 version of the McAfee Scan Engine was susceptible to a buffer overflow when scanning malformed LHa files. An alteration to the configuration of the Scan Engine issued (March 1, 2005) with the 4436 DAT file was made to eliminate the vulnerability within the 4320 Scan Engine. The McAfee 4400 engine (issued November 2004) does not have this vulnerability.

Products affected: *Scan Engine v.4320* – any McAfee point products still using the 4320 engine and DAT version less than 4436.

The following McAfee products and suites may include the vulnerable engine (4320).

McAfee Consumer Products:

- McAfee InternetSecurity Suite
- VirusScan (all versions)
- VirusScan Professional

McAfee SMB and Enterprise Products:

- Active Mail Protection
- Active Threat Protection
- Active Virus Defense SMB Edition
- Active VirusScan SMB Edition
- GroupShield for Exchange
- GroupShield for Exchange 5.5
- GroupShield for Lotus Domino
- GroupShield for Mail Servers with ePO
- LinuxShield
- Managed VirusScan
- NetShield for Netware
- PortalShield for Microsoft SharePoint
- SecurityShield for Microsoft ISA Server
- Virex
- VirusScan ASaP
- VirusScan Command Line
- VirusScan® Enterprise 8.0i
- VirusScan for NetApp
- WebShield Appliances
- WebShield SMTP

Recommendations

For McAfee Consumer Customers:

McAfee strongly recommends customers to download and apply the latest .DAT files and the latest Scan Engine (v.4400). No action is required if the Scan Engine version is 4400 or the DAT version is 4436 (issued March 1 2005) or higher. Consumers can update their software by right-clicking on their system tray icon (white M on Red background) and selecting “Updates”. More information is available at: http://ts.mcafeehelp.com/faq3.asp?docid=378097.

For McAfee SMB and Enterprise Customers:

To address the above vulnerabilities, McAfee strongly recommends customers to download and apply the latest .DAT files and the latest Scan Engine (v.4400). No action is required if the Scan Engine version is 4400 or the DAT version is 4436 (issued March 1 2005) or higher. We urge all customers to verify that the 4436 DAT [or higher] and/or the 4400 Scan Engine have been installed and deployed.

These files are available at:

http://www.mcafeesecurity.com/us/downloads/updates/default.asp

Knowledge base article KB40234 also discusses this issue and is available at:

https://knowledgemap.nai.com/phpclient/homepage.aspx

Please note: it is no longer necessary to log into Service Portal to search our Knowledge Base, just click the ‘Knowledge’ link on the left menu.

How do I check Engine & DAT Versions within Enterprise Products?

- *ePolicy Orchestrator Repositories* - From the Management Console, click on Repository, Software Repositories, Master.
- *GroupShield for Exchange* - Open GUI, Product Versions are listed on opening screen.
- *GroupShield for Exchange 5.x* - Open GUI, Click on Versions tab.
- *GroupShield for Lotus Domino* - Open GUI, Product Versions are listed on opening screen.
- *LinuxShield* - Open GUI, Product Versions are listed on opening screen.
- *Managed VirusScan* - Right-mouse click on VirusScan in the systray, select about
- *Managed VirusScan Online Admin* - From the admin login reporting page, Click View, Reports/All Computers. (note: All version 3 users have the 4400 Engine)
- *NetShield for Netware* - Right-mouse click on Shield in the systray, select about
- *PortalShield for Microsoft SharePoint* - Open GUI, Product Versions are listed on opening screen.
- *ProtectionPilot Repositories* - Click on Server, click on Repository Tab
- *SecurityShield for Microsoft ISA Server* - Open GUI, Product Versions are listed on opening screen.
- *Virex 7.5* - From within Virex application, select about Virex from the Virex menu.
- *Virex 6.2* - Double-click on the green Virex emblem in the Control Panel.
- *VirusScan (all versions)* - Right-mouse click on VirusScan in the systray, select about
- *VirusScan Professional* - Right-mouse click on VirusScan in the systray, select about
- *VirusScan ASaP* - Right-mouse click on VirusScan in the systray, select about
- *VirusScan Command Line* - From a DOS Command Prompt, Run Scan.exe /version
- *VirusScan for NetApp* - Right-mouse click on VirusScan in the systray, select about
- *VirusScan® Enterprise 8.0i* - Right-mouse click on VirusScan in the systray, select about
- *WebShield Appliances* - Select the System status page.
- *WebShield SMTP* - Select the System status page.

Other References

Additional information on this issue may be found at: http://xforce.iss.net/xforce/alerts/id/190

Acknowledgements

McAfee, Inc. wishes to thank Alex Wheeler of the ISS X-Force for the discovery of these vulnerabilities and for working with us to protect our customers.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com