

[NT] Remote DoS in GFI MailEssentials (Microsoft HTML Parser)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0013.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 01/04/05

To: list@securiteam.com

Date: 4 Jan 2005 13:02:49 +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>

Remote DoS in GFI MailEssentials (Microsoft HTML Parser)

SUMMARY

<<http://www.gfi.com>> GFI MailEssentials for Exchange/SMTP "offers SPAM protection and email management at server level. GFI MailEssentials offers a fast set-up and a high SPAM detection rate using Bayesian analysis and other methods – no configuration required, very low false positives through its automatic whitelist, and the ability to automatically adapt to your email environment to constantly tune and improve SPAM detection. GFI MailEssentials also adds email management tools to your mail server: disclaimers, mail archiving and monitoring, Internet mail reporting, list server, server-based auto replies and POP3 downloading".

CSIS has discovered a flaw in GFI MailEssentials 9 and 10.x and GFI MailSecurity 8.x where a specially crafted HTML email causes the products to stop processing, resulting in emails getting stuck in the IIS/Exchange queues.

DETAILS

Affected Products:

* GFI MailSecurity 8.x

Securiteam: [NT] Remote DoS in GFI MailEssentials (Microsoft HTML Parser)

- * GFI MailEssentials 9
- * GFI MailEssentials 10.x

The problem lies in a Microsoft HTML library that is made use of by a GFI library, common to GFI MailSecurity and GFI MailEssentials.

A malicious user can exploit this flaw and craft an e-mail containing a specially crafted javascript. When the e-mail containing the javascript is received by MailEssentials, it will be processed resulting in a DoS. The mail will reside in the queues until it's manually removed. If the server is rebooted without removing the affected mail from the queues, the same mail gets processed again and again and a new DoS will occur. MailEssentials will not process any other in- or outbound e-mails until this mail is completely removed from the bad mail queue. This is a ugly scenario since you'll end up looking for a needle in a haystack.

CSIS would like to underline that this flaw is really a result of a bug in Microsoft HTML parser. As such, this problem is not directly related to GFI. We suspect other products are vulnerable as well.

Impact:

This is a remote DoS. Leaving no trace, no warnings and no indication of which e-mail causing the problem.

Solution:

A fix has been released:

GFI MailEssentials 10.x –

ftp://ftp.gfi.com/patches/ME10_PATCH_20041220_01.zip

ftp://ftp.gfi.com/patches/ME10_PATCH_20041220_01.zip

GFI MailEssentials 9 –

ftp://ftp.gfi.com/patches/me9_PATCH_20041220_01.zip

ftp://ftp.gfi.com/patches/me9_PATCH_20041220_01.zip

GFI MailSecurity 8.x –

ftp://ftp.gfi.com/patches/MSEC8_PATCH_20041220_01.zip

ftp://ftp.gfi.com/patches/MSEC8_PATCH_20041220_01.zip

It's strongly recommended to apply these patches as soon as possible. Also it would be wise to set up an alert mechanism monitoring number of mails in queue. CSIS also recommend using the GFI monitor function to see if mails gets processed at regular intervals.

Running on Microsoft Windows 2000 Server with all relevant patches installed.

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1312>

CAN-2004-1312

Links:

For more information about the patches see GFI KB article:

[NT] Remote DoS in GFI MailEssentials (Microsoft HTML Parser)

Securiteam: [NT] Remote DoS in GFI MailEssentials (Microsoft HTML Parser)

<<http://kbase.gfi.com/showarticle.asp?id=KBID002249>>
<http://kbase.gfi.com/showarticle.asp?id=KBID002249>

ADDITIONAL INFORMATION

The information has been provided by <mailto:kruse@krusesecurity.dk>
Peter Kruse.

The original article can be found at:
<<http://www.csis.dk/default.asp?m=1&a=194>>
<http://www.csis.dk/default.asp?m=1&a=194>

=====

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.