

Received: from navgwout.symantec.com ([198.6.49.12])
by mx1.comcept.net (SMSSMTP 4.0.0.59) with SMTP id M2004062211540303463
for <MUNGED@terabyte.net>; Tue, 22 Jun 2004 11:54:03 -0400
Received: from navgwout.symantec.com (localhost [127.0.0.1])
by navgwout.symantec.com (8.11.7p1+Sun/8.11.7) with SMTP id i5MFs3125333
for <MUNGED@terabyte.net>; Tue, 22 Jun 2004 08:54:03 -0700 (PDT)
Received: from uscu-smtpob01-1.symantec.com ([155.64.74.130])
by navgwout.symantec.com (SAVSMTP 3.1.2.35) with SMTP id M2004062208540227793
for <MUNGED@terabyte.net>; Tue, 22 Jun 2004 08:54:02 -0700
In-Reply-To: <6.1.1.1.2.20040620191745.03c19d68@mail.terabyte.net>
To: "Brian S. Bergin" <MUNGED@terabyte.net>
Cc: MUNGED <MUNGED@symantec.com>,
MUNGED <MUNGED@symantec.com>
Subject: RE: Fw: double encoded MIME messages
MIME-Version: 1.0
X-Mailer: Lotus Notes Release 6.0.2CF1 June 9, 2003
From: MUNGED <MUNGED@symantec.com>
Message-ID: <0FA7DC7A96.0C407700-0N86256EBB.00511E5A-86256EBB.005757E5@symantec.com>

Date: Tue, 22 Jun 2004 10:54:01 -0500
X-MIMETrack: Serialize by Router on USCU-SMTP0B01-1/GLOBE-ADMIN/SYMANTEC(602CF1HF35
| July
14, 2003) at 06/22/2004 08:54:02 AM
Serialize complete at 06/22/2004 08:54:02 AM
Content-Type: text/plain; charset="US-ASCII"

Brian,

I don't see the departure from what I originally said and have said all along?

Had we, during our coordination, determined this to be a product vulnerability issue we would have responded to it as such. However, since our coordination does not show it to be a vulnerability issue, the Product Security Team is not going to handle it as such. I am still providing you with the response we did coordinate to address your concerns.

After much internal coordination, we don't see this issue as a product vulnerability.

Your issue is a bounced message exhibiting embedded MIME behavior. When some mail servers refuse to accept an email, in this instance one that contained a virus attachment, they return the complete mime-encoded email message in the bounce message as in your case. The message body of the "bounce" email contains an embedded text copy of the actual complete multipart MIME message. If it were a standalone message, this embedded message would also contain attachments. However, within the singlepart plaintext message structure of the "bounce" message, the original multipart mime message is just a block of mime-encoded text.

These singlepart plaintext mime messages do not contain attachments, and do not represent a vulnerability since there is no way for a viral payload to be executed as strictly a text message. The viral attachment portion of the "bounced" message has been stripped. Because of this, some of our products, by default, do not attempt to decode single part plaintext message bodies prior to scanning for viruses, although there may be a way to configure them so they will. Doing so, in many cases, does have a adverse impact on false positive mime identification (identifying mime-like text as a mime message) and message throughput. Although, in your testing you found that not to have an impact, our testing and support experience has shown different results.

Agree that some of our antivirus scanning products can/will still detect the message as being viral even if it does not, in fact, contain a viral

payload at this point. Depending on their configuration in the "layered" defense of a network, the products can separate the message parts, separating the top-level mime headers from the message body. The message body is then scanned as an independent entity, not as part of an entire message. The scanner will take the block of text, scan it, detect what appears to be a mime message, then decode and scan that although the message in its complete form would not have been decoded and no attachment would have been displayed. During this scan, a virus detection could occur, based on pattern-matching, even though there is no viral attachment payload which can be executed by the end user's client. So, yes there was a virus attachment in the original message but at this point in the "bounce" message, it is merely plaintext, not executable.

Symantec does not slipstream fixes to reported security issues quietly into our products. We are a responsible disclosure company. Our vulnerability disclosure policy is clearly stated on our security web page, <http://www.symantec.com/security>.

Our product engineers are constantly working to improve the scanning/detection capabilities of our products. As we identify issues that have or will potentially have impact on our products (all, not just those security-related) we plan solutions for those issues and work them into our product line at the points where they can provide the most protection for our customers without causing undue or unnecessary performance concerns. That is normal product enhancement and updating, not slipstreaming.

We are taking your comments on the knowledge base article and on this issue in general and working them into our support planning. In fact, the concerns you voiced about not being able to configure the dec settings in SAVCE 8.x have been submitted as a needed MR update.

Brian, once again, I regret the length of time it has taken me to get back to you on this issue. That is mostly my fault as I stated previously.

This is not a product vulnerability issue and we do not intend to report it as a product vulnerability. It is a support issue compounded possibly by some confusion with the behavior and makeup of the bounce messages you are seeing. Those we do intend to address.

SIGNATURE MUNGED