

[NT] ZoneLabs SMTP Processing Buffer Overflow (RCPT TO)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0059.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/22/04

To: list@securiteam.com

Date: 22 Feb 2004 15:03:59 +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>

ZoneLabs SMTP Processing Buffer Overflow (RCPT TO)

SUMMARY

<<http://www.zonelabs.com>> ZoneLabs provides a suite of desktop firewall products. Products in this suite such as ZoneAlarm analyze incoming and outgoing email messages for malicious or otherwise abnormal content. When ZoneAlarm examines outgoing email messages a buffer overflow condition is presented when the destination email address is retrieved from the message. An attacker can exploit this vulnerability to elevate his privileges to SYSTEM on any machine protected by a vulnerable ZoneLabs product. This vulnerability can also be exploited remotely if an attacker can manipulate the protected system into sending an outgoing email message.

DETAILS

A stack based buffer overflow vulnerability within vsmon.exe can be exploited to execute code with the context of the SYSTEM account. The vulnerability exists within the component responsible for processing the RCPT TO command argument. By specifying a large argument to the RCPT TO command an internal stack based buffer can be overflowed within the TrueVector Internet Monitor (vsmon.exe) process.

Securiteam: [NT] ZoneLabs SMTP Processing Buffer Overflow (RCPT TO)

Vendor Status:

ZoneLabs was contacted and within only a few days they produced an update to eliminate this vulnerability within their products. We would like to give special recognition to the responsiveness of ZoneLabs in creating a fix to protect their customers.

A patch for this vulnerability can be found at:

<<http://download.zonelabs.com/bin/free/securityAlert/8.html>>

<http://download.zonelabs.com/bin/free/securityAlert/8.html>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mmaiffret@EEYE.COM> Marc Maiffret.

=====

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.