

Securiteam: [NEWS] Multi-Vendor AntiVirus Gateway Image Inspection Bypass (data:)

[NEWS] Multi-Vendor AntiVirus Gateway Image Inspection Bypass (data:)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0049.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/11/05

To: list@securiteam.com

Date: 11 Jan 2005 13:06:27 +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>

Multi-Vendor AntiVirus Gateway Image Inspection Bypass (data:)

SUMMARY

A vulnerability has been discovered which allows a remote attacker to bypass anti-virus (as well other security technologies such as IDS and IPS) inspection of HTTP image content. By leveraging techniques described in RFC 2397 for base64 encoding image content within the URL scheme. A remote attacker may encode a malicious image within the body of an HTML formatted document to circumvent content inspection.

DETAILS

The source code at the URL

<<http://www.securiteam.com/exploits/5EP0M0KE0W.html>>

<http://www.securiteam.com/exploits/5EP0M0KE0W.html> will by default create a JPEG image that will attempt (and fail without tweaking) to exploit the Microsoft MS04-028 GDI+ vulnerability. The image itself is detected by all AV gateway engines tested (Trend, Sophos and McAfee), however, when the same image is base64 encoded using the technique described in RFC 2397 (documented below), inspection is not performed and is delivered rendered by the client.

Securiteam: [NEWS] Multi-Vendor AntiVirus Gateway Image Inspection Bypass (data:)

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.