

[REVS] Exploiting WDM Audio Drivers

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Jan 2008 19:41:54 +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>

Exploiting WDM Audio Drivers

SUMMARY

For those researchers who are interested in the driver security and also for driver writers, the paper "Exploiting WDM Audio Drivers" has been released.

This paper explains an attack vector inherent to certain WDM audio drivers running on Windows Vista, XP, 2000 and 2003. Successful exploitation could lead to local escalation of privileges.

The paper also covers the interesting case of es1371mp.sys, a vulnerable WDM driver that can be automatically installed through Windows Update, on systems with Ensoniq PCI 1371 based SoundCards (Certain VMware products emulate a soundcard of this type).

DETAILS

Conclusion:

Writing secure drivers (secure code really) is not an easy task, there are dozens of important concepts involved, moreover a strong knowledge of the OS you are programming for is highly recommended. There is a method for modeling risks in complex systems known as the Swiss Cheese Theory . This

[REVS] Exploiting WDM Audio Drivers

model is widely used in Aeronautical Industry and is also suitable for analyzing risk factors within the IT security Industry. Imagine several slices of Swiss Cheese, with all those tiny holes, each of these slices is a layer that is potentially avoiding that the threat can go forward through the holes, finally reaching the last stage of system. If all the layers fail, the whole system gets compromised and you may face an airplane crashing, a building collapsing or an attacker taking the control of your computer. This paper is the story of what happens when all those "cheese" layers fails.

ADDITIONAL INFORMATION

The information has been provided by Ruben Santamarta.

The original article can be found at:

http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=fileinfo&id=54
http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=fileinfo&id=54

=====

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@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

=====

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.