

[Full-disclosure] Defeating Microsoft WGA Validation Check

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-05/0538.html>

From: Debasis Mohanty (mail_at_hackingspirits.com)

Date: 05/23/05

To: <full-disclosure@lists.grok.org.uk>

Date: Mon, 23 May 2005 15:16:22 +0530

There is lot of hype about WGA (Windows Genuine Advantage) when Microsoft builds functionality in its few of the public beta products to conduct a genuine product check before the product gets installed. MS products or tools with WGA check enabled can only be installed on a valid / genuine copy of MS Windows XP. In case it is a pirated copy then the product denies to install.

If you are aware of Microsoft WGA validation then you can directly jump in to the PoC section otherwise it is advisable to read on WGA and what it does before reading the PoC.

To know more about WGA, refer to the following Microsoft link:

<http://www.microsoft.com/genuine/downloads/FAQ.aspx?displaylang=en>

Defeating Microsoft WGA Validation Check – Proof of Concept (PoC)

This PoC explains how Microsoft WGA validation check can be defeated and any Microsoft product with the WGA validation feature can be run and installed on machines running pirated copy of Windows XP. To bypass WGA validation check, one can run "GenuineCheck.exe" file on a machine running a copy of an authentic Windows XP for generating a key code. This key code generated on the machine running genuine copy of Win XP can be used to circumvent the WGA check on the machine running a pirated copy of Win XP.

A detailed approach can be downloaded from the following link –

Full-Disclosure: [Full-disclosure] Defeating Microsoft WGA Validation Check

<http://www.hackingspirits.com/vuln-rnd/defeating-wga-check.zip>

Microsoft in its reply to my mail specified that "The generated code is partly made up of a timestamp, which would prevent use after a short period". However, I checked this on a pirated copy of Windows XP Pro and installed couple of public beta products and tools for testing purpose. They are still up and running since past 1.5 months.

Incase, anyone is going to try this out on their pirated versions of Win XP then do let me know if the installed product make noise after certain time period.

* Debasis Mohanty

* www.hackingspirits.com <<http://www.hackingspirits.com/>>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>