

Exploit Allows Windows XP Piracy

By *srlinuxx*

Created *24/05/2005 - 3:51am*

Submitted by srlinuxx on Tuesday 24th of May 2005 03:51:23 AM Filed under [Microsoft](#) [1]

There's a major chink in Microsoft's Windows XP anti-piracy armor, although Windows users are not at risk of security attacks.

A security researcher in India has discovered an uncomplicated and easy-to-exploit weakness in Microsoft Corp.'s WGA (Windows Genuine Advantage), an anti-piracy initiative that checks whether consumer and small-business customers are running legitimately licensed copies of Windows XP.

Debasis Mohanty, a private vulnerability researcher and analyst of malicious programs, published a detailed proof-of-concept demonstration to show how the WGA validation check can be defeated to generate key codes for use on illegal copies of Windows XP.

Mohanty's findings come as the world's largest software maker prepares a mandatory rollout of the program.

Microsoft has been testing the Genuine Advantage program through its Download Center, where users are urged to validate their copies of XP before obtaining certain software updates, patches and fixes.

If users decide against validating, they are still allowed to obtain the requested downloads, but later this summer updates will only be pushed out to valid copies. Security updates will not require validation, even after WGA goes mandatory.

A Microsoft spokesperson on Monday confirmed Mohanty's findings but insisted that the weakness presented no real threat to the company's attempts to strangle software pirates.

The spokesperson said there were no plans to modify the way WGA works, even after Mohanty's public demonstration, which was posted on a high-profile security mailing list.

[Full Story](#) [2].

[Microsoft](#)

Source URL: <http://www.tuxmachines.org/node/1043>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/62>

[2] <http://www.eweek.com/article2/0,1759,1819231,00.asp>