# Hotmail in hot water over password flaw, rushes fix

April 28 2012, by Nancy Owano

Hackers tried to get the best of Hotmail by figuring out how to reset Hotmail user passwords for e-mail accounts this month. Locking hotmail users out of their own accounts when trying to key in their passwords was something like a bad-dream scenario, trying to open your front door only to find your key does not work and thieves are inside. This could have turned into a big-time nightmare if Microsoft, after being notified of the weakness, had not rushed out a patch for its troubled password reset system. The Redmond company reportedly closed the loophole, so that hackers trying to manipulate data would now get an error message.

The fix was issued after information about the bug was actively publicized online. According to security watching reports, information about the bug and how to pull the password caper off spread "like wildfire" and some mischief-makers were offering to hack Hotmail accounts for twenty dollars a shot. They realized it was possible to manipulate data passed between a user and Hotmail servers in such a way that could give them control over an account,

The flaw in the password reset functionality allowed a remote attacker to reset the Hotmail/MSN password with the attacker's own values, according to a notice dated April 26 by Vulnerability Lab senior researcher Benjamin Kunz Mejri.

The bug basically involved the way Hotmail handled (or didn't) the information that must be processed when a user wants to reset the Hotmail password.

Peter Bright, writing in *ars technica*, explained that Hotmail's password reset system uses a token system to ensure that only the account holder can reset the password. The weakness was in the validation of the tokens, a weakness allowing attackers to reset passwords of any account.

Vulnerability Lab researcher Mejri explained, "The token protection only checks if a value is empty then blocks or closes the web session. A remote attacker can, for example bypass the token protection with values "+++)-". Successful exploitation results in unauthorized MSN or Hotmail account access. An attacker can decode CAPTCHA & send automated values over the MSN Live Hotmail module."

Email user stats are not uniform; the numbers set forth of Hotmail users vary, somewhere between an estimated 350 million and 360 million. Sophos and other security sites say it is not known how many of these users experienced incidents over their Hotmail accounts. Those who may have fallen victim would have known if they found they were locked out of their Hotmail accounts. Hackers would know that particular game was over in their getting an error message upon trying to sabotage the data exchange. Microsoft, addressing the incident, confirmed the fix and said "there is no action for customers, as they are protected."

Citation: Hotmail in hot water over password flaw, rushes fix (2012, April 28) retrieved 23 April 2024 from https://phys.org/news/2012-04-hotmail-hot-password-flaw.html