heise online IT news, features and forums at heise online UK

28 March 2008, 13:23

Black Hat: new operating systems security metric

At the **Black Hat Security Conference[1]** currently taking place in Amsterdam, researchers from the Zurich ETH (Swiss Federal Institute of Technology) have reported a new model for determining the security of operating systems. They don't just count the number of holes and how critical they are, but also determine what they call the zero-day patch rate. This indicates the ability of a vendor to make a patch available on the day a vulnerability becomes known. In order to stay independent of vendor information, they looked at many independent sources including Secunia, Milw0rm, The Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVD) and CVE.

Stefan Frei, Bernard Tellenbach and Bernhard Plattner of the Communications Systems Group of the ETH explain their method in **"0-Day patch - Exposing Vendors (In)Security Performance"[2]** (PDF file) using Microsoft and Apple operating systems as examples. They base their assessments on experience over the last six years. In addition to the zero-day patch rate, the authors also graph the availability of patches 30, 90 and 180 days after a vulnerability becomes known. It appears that both Microsoft and Apple take longer to provide a patch in the run-up to the issue of a new version of their operating system or a service pack. These releases evidently tie up substantial resources, which are less available for developing patches.

The researchers come to the further conclusion that the number of Microsoft's open vulnerabilities has now stabilised, whereas the trend is the other way round with Apple. Apple has in fact already overtaken Microsoft, averaging a greater number of open vulnerabilities. The researchers say the results do not support the widespread assumption that Apple computers are naturally more secure. The **latest Apple update[3]** for Mac OS X eliminated 46 vulnerabilities, 13 of them in the Safari browser alone.

See also:

- **0-Day Patch - Exposing Vendors (In)Security Performance[4]**, study by Stefan Frei, Bernard Tellenbach and Bernhard Plattner

(**mba[5]**)

URL of this Article:
http://www.heise-online.co.uk/news/110423

Links in this Article:
[1] http://www.blackhat.com/html/bh-europe-08/bh-eu-08-speakers.html#Frei
[2] http://www.techzoom.net/papers/blackhat_0day_patch_2008.pdf
[3] http://www.heise-online.co.uk/news/Apple-security-update-fixes-46-bugs--/110356

[4] http://www.techzoom.net/papers/blackhat_0day_patch_2008.pdf
[5] mailto:mba@heise-online.co.uk