BIZ & IT —

32TB of Windows 10 beta builds, driver source code leaked [Updated]

Dump appears to contain components normally only shared with partners.

PETER BRIGHT - 6/24/2017, 2:15 AM

Rural Learning Center

Enlarge

32TB of unreleased, private Windows 10 builds, along with source code for certain parts of the driver stack, have been leaked to BetaArchive, reports The Register.

The dump appears to contain a number of Windows 10 builds from the development of codenamed Redstone 2. Redstone 2 was released earlier this year, branded as the Creators Update.

Some of these builds are built for 64-bit ARM chips, and some are said to include private debug symbols. Microsoft routinely releases debug symbols for Windows; the symbols contain additional information not found in the compiled Windows binaries that helps software developers identify which functions their code is calling. The symbols normally released are public symbols; while they identify many (though not all) functions and data structures, they don't contain information about each function's variables or parameters. The private symbols, in contrast, contain much more extensive information, giving much more insight into what each piece of code is doing and how it's doing it.

The leak is also described as containing a source code package named the "Shared Source Kit." This is a package of source code for things like the USB, storage, and Wi-Fi stacks, and the Plug-and-Play

system. It isn't the core operating system code (part of which leaked in 2004) but rather contains those parts of the driver stack that third parties have to interact most intimately with.

Finally, the leak is said to contain versions of the Windows 10 "Mobile Adaptation Kit," which is used to assemble system images for Windows on phones.

The source of the leaks is currently unknown, though speculated to have been Microsoft's own systems. The Register and other publications suggest that the source code leak will be of grave security consequence; that the mere publication of parts of the Windows source will unleash a barrage of attacks. The Windows 2000 code leak did not appear to result in a spate of exploits, and today's Windows code is likely to be in rather better shape than that of 2004.

In this writer's view, the apparent penetration of Microsoft's systems is of far more concern. In March, we received an unconfirmed report that Microsoft's build systems had been hacked. If such a hack did indeed take place then leaks of internal builds and build-related tools might well be the consequence. However, it's also possible that the source of the leaks was some close Microsoft partner; OEM partners receive more builds than are distributed publicly, and so it's possible that one of them might be to blame.

Update: BetaArchive says that it has deleted the Shared Source Kit from its servers in response to The Register's article. It also claims that the private beta builds come from an array of sources, not any one particular leak. BetaArchive also says that the leaks are unlikely to be related to arrests made in the UK of two men over plans to hack into Microsoft.

READER COMMENTS 60

SHARE THIS STORY

Unsolved Mortal Kombat Mysteries With Dominic Cianciolo From NetherRealm Studios

mysteries of the Mortal Kombat universe. Thank you to r/MortalKombat on reddit and the Ars Technica community for providing questions! Directed and Produced by Justin Wolfson Edited by Ron Douglas

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars