Security and DRM Leftovers

By *Roy Schestowitz*
Created *26/09/2021 - 11:44pm*
Submitted by Roy Schestowitz on Sunday 26th of September 2021 11:44:20 PM Filed under Security [1]

- **Azure OMIGOD Flaw Under Attack [2] [Ed: Microsoft Azure as de facto back door in Linux [3]]**

- **Microsoft Azure OMI Vulnerabilities Are Being Exploited [4]**

- **Security experts weigh in on Microsoft Azure security holes [5] [Ed: Security experts would never touch Azure]**

- **Microsoft asks Azure Linux admins to manually patch OMIGOD bugs [6]**

- **Apple warns of arbitrary code execution zero-day being actively exploited on Macs [7]**

  Apple has warned iPhone and Mac users it's aware of security bugs in its software that are being actively exploited.

  First off, the iGiant thanked Google for spotting CVE-2021-30869 in macOS Catalina. It's a nasty flaw, as it's in the XNU kernel at the heart of Apple's operating systems including macOS and iOS.

  As Apple's advisory explains, "a malicious application may be able to execute arbitrary code with kernel privileges" by exploiting this security hole. Thus, malware running on a system can use the bug to take total control. The fruit-themed company says the flaw existed thanks to

a "type confusion issue" that was sorted out "with improved state handling."

- **Microsoft WPBT flaw lets hackers install rootkits on Windows devices [8] [Ed: Even Microsoft-connected sites such as this know that Windows is inadequate for security]**

  Security researchers have found a flaw in the Microsoft Windows Platform Binary Table (WPBT) that could be exploited in easy attacks to install rootkits on all Windows computers shipped since 2012.

- **Is it OK to use stolen data? What if it's scientific research in the public interest? [9]**

  There's a fine line between getting hold of data that may be in the public interest and downright stealing data just because you can. And simply because the data is out there ? having been stolen by online intruders and then leaked ? does not mean it is right to use it.

  A paper published in Nature Machine Intelligence this week is an effort to help guide data scientists and researchers through the ethical dilemmas which present themselves when considering using information obtained from data breaches.

- **A new zero-day is being exploited to compromise Macs (CVE-2021-30869) [10]**

  Flagged by researchers Erye Hernandez and Clément Lecigne of Google?s Threat Analysis Group and Ian Beer of Google Project Zero, the vulnerability is a type confusion issue found in XNU, the kernel of Apple?s macOS and iOS operating systems.

- **Plug critical VMware vCenter Server flaw before ransomware gangs start exploiting it (CVE-2021-22005) [11]**

  ?This vulnerability can be used by anyone who can reach vCenter Server over the network to gain access, regardless of the configuration settings of vCenter Server,? the company noted.

- **Apple* and John Deere* shareholders file resolutions questioning their anti-repair stances | U.S. PIRG [12]**

  Shareholders press these leading Right to Repair opponents to explain themselves as regulatory pressure mounts

- **Ransomware attacks reach disturbing levels** **[13]**

- **Ransomware attacks have reached 'stratospheric' levels** **[14]**

- **Ransomware attacks reach 'stratospheric' levels finds new research** **[15]**

Security

Source URL: http://www.tuxmachines.org/node/156125

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://duo.com/decipher/azure-omigod-flaw-under-attack
[3] http://techrights.org/2021/09/16/microsoft-azure-bug-doors/
[4] https://mytechdecisions.com/it-infrastructure/microsoft-azure-omi-vulnerabilities-are-being-exploited/
[5] https://securitybrief.com.au/story/security-experts-weigh-in-on-microsoft-azure-security-holes
[6] https://www.bleepingcomputer.com/news/microsoft/microsoft-asks-azure-linux-admins-to-manually-patch-omigod-bugs/
[7] https://www.theregister.com/2021/09/24/apple_zero_day/
[8] https://www.bleepingcomputer.com/news/security/microsoft-wpbt-flaw-lets-hackers-install-rootkits-on-windows-devices/
[9] https://www.theregister.com/2021/09/17/unethical_data_research/
[10] https://www.helpnetsecurity.com/2021/09/24/cve-2021-30869/
[11] https://www.helpnetsecurity.com/2021/09/22/cve-2021-22005/
[12] https://uspirg.org/blogs/blog/usp/apple-and-john-deere-shareholders-file-resolutions-questioning-their-anti-repair
[13] https://securitybrief.co.nz/story/ransomware-attacks-reach-disturbing-levels
[14] https://www.itproportal.com/news/ransomware-attacks-have-reached-stratospheric-levels/
[15] https://www.continuitycentral.com/index.php/news/technology/6688-ransomware-attacks-reach-stratospheric-levels-finds-new-research