Virtual machine escape fetches $105,000 at Pwn2Own hacking contest [updated]

By Dan Goodin

Published: 2017-03-17 · Archived: 2026-04-05 21:15:32 UTC

Contestants at this year's Pwn2Own hacking competition in Vancouver just pulled off an unusually impressive feat: they compromised Microsoft's heavily fortified Edge browser in a way that escapes a VMware Workstation virtual machine it runs in. The hack fetched a prize of $105,000, the highest awarded so far over the past three days.

According to a Friday morning tweet from the contest's organizers, members of Qihoo 360's security team carried out the hack by exploiting a heap overflow bug in Edge, a type confusion flaw in the Windows kernel and an uninitialized buffer vulnerability in VMware, contest organizers reported Friday morning on Twitter. The result was a "complete virtual machine escape."

"We used a JavaScript engine bug within Microsoft Edge to achieve the code execution inside the Edge sandbox, and we used a Windows 10 kernel bug to escape from it and fully compromise the guest machine," Qihoo 360 Executive Director Zheng Zheng wrote in an e-mail. "Then we exploited a hardware simulation bug within VMware to escape from the guest operating system to the host one. All started from and only by a controlled a website."

Virtual machines are vital to the security of individuals and large organizations everywhere. In server hosting environments, they're used as a container that prevents one customer's data and operating system from being accessed by other customers sharing the same physical server. Virtual machines such as the VMware Workstation hacked Friday are also used on desktop computers to isolate untrusted content. Should the guest operating system be compromised through a drive-by browsing exploit or similar attack, the hackers still don't get access to data or operating system resources on the host machine.

Any hack that can break out of a widely used virtual machine is generally considered significant. The one described Friday is made all the more impressive because it works by exploiting Edge, which is regarded among security professionals as one of most challenging browsers to exploit. Typically, such remote-code exploits require two or more vulnerabilities to be exploited in unison. The requirement appears to be why the Qihoo team combined the heap overflow exploit with the Windows kernel hack. The description sets up a scenario in which malicious websites can not only compromise a visitor's virtual machine, but also the much more valuable host machine the VM runs on. At last year's Pwn2Own, contestants didn't attempt to target VMWare, an indication reliable exploits were probably worth more than the $75,000 prize that was offered at the time.
