Riot addresses “kernel-level driver” concerns with expanded bug bounties

Enlarge / Artist’s conception of hackers lining up for these new bug bounties.

reader comments

59 with 51 posters participating

Share this story

Last week, we took a look at the new Vanguard anti-cheat system being used in Riot’s *Valorant* and the potential security risks of the kernel-level driver it utilizes. Now, in an effort to allow “players to continue to play our games with peace of mind,” Riot says it is “putting our money where our mouth is” with an expanded bug bounty program, offering more money for the discovery of Vanguard vulnerabilities. Bug bounties aren’t new to the gaming industry or even to Riot Games, which says it has paid out nearly $2 million in such rewards since launching its bounty program in 2016. But Riot is now offering “even higher bounties” of up to $100,000 specifically for the discovery of “high quality reports that demonstrate practical exploits leveraging the Vanguard kernel driver.”

The largest bounties in Riot’s newly expanded program are available to attacks that are able to exploit the Vanguard driver to run unauthorized code at the kernel level—something of a nightmare scenario that could give an attacker full, low-level access to a machine—but exploits that merely provide

“unauthorized access to sensitive data” will also be rewarded. The bounties apply to network-based attacks that need no user interaction, vulnerabilities that require user action (like clicking on a malicious link), and exploits that require “guest user” access to the system itself, in declining order of potential reward.

Offering bug bounties is an attempt to skew the incentive structure for potential Vanguard attackers, making it more lucrative to report flaws than to exploit them for use by cheating programs or hacking tools. Riot anti-cheat lead Paul Chamberlain said a similar issue of incentives was behind Riot’s decision to use a kernel-level driver for Vanguard in the first place.

Beating a kernel-level driver “requires a different (more strenuous) approach from cheat developers to attack,” Chamberlain told Ars. “For cheat developers operating at the kernel level, they need to work around the restrictions Microsoft places on kernel level software. This extra work reduces the incentives for cheat developers because their cheats become harder to make, less convenient for players to install, and just overall less profitable to sell.

“We don’t expect that any protection will remain unbreached forever, but Vanguard’s protections are strong, and as cheat developers’ tactics evolve, so will ours.”

Earning player trust

In announcing the new bug bounties, a group of high-level Riot security employees wrote that they “understand the decision to run the driver component in kernel-mode can raise concerns.” That said, they also want to reassure players that “we would never let Riot ship anything if we weren’t confident it treated player privacy and security with the extreme seriousness they deserve.”

The statement reiterates that while the signed kernel-level driver runs at start-up “to prevent loading cheats prior to the client initialization,” a user-level client “handles all of the anti-cheat detections while a game is running.” At that point, the user-level client uses the driver “to validate memory and system state and to make sure the client has not been tampered with.” The driver itself “does not collect or send any information about your computer back to us,” they wrote.

“We’d never let Riot ship something we couldn’t stand behind from a player-trust perspective (not that we think Riot would ever try),” Riot’s security representatives wrote. “Players have every right to question and challenge us, but let’s be clear—we wouldn’t work here if we didn’t deeply care about player trust and privacy and believe that Riot feels the same way. We’re players just like you, and we wouldn’t install programs on our computer that we didn’t have the utmost confidence in.”

https://arstechnica.com/?p=1669539