A Google security analyst has found a serious weakness in Blizzard games that could enable remote assailants to run malicious code on gamers' PCs.

Played each month significantly a billion clients—World of Warcraft, Overwatch, Diablo III, Hearthstone and Starcraft II are famous internet diversions made by Blizzard Entertainment.

To play Blizzard amusements web-based utilizing web programs, clients need to introduce a diversion customer application, called 'Snowstorm Update Agent,' onto their frameworks that run JSON-RPC server over HTTP convention on port 1120, and "acknowledges charges to introduce, uninstall, change settings, refresh and other support related alternatives."

Google's Project Zero team researcher Tavis Ormandy discovered that the Blizzard Update Agent is vulnerable to a hacking technique called the "DNS Rebinding" attack that allows any website to act as a bridge between the external server and your localhost.

Just last week, Ormandy revealed a similar vulnerability in a popular Transmission BitTorrent app that could allow hackers to remotely execute malicious code on BitTorrent users' computers and take control of them.
By simply creating a DNS entry to bind any attacker-controlled web page with localhost (127.0.0.1) and tricking users into visiting it, hackers can easily send privileged commands to the Blizzard Update Agent using JavaScript code.

Although a random website running in a web browser usually cannot make requests to a hostname other than its own, the local Blizzard updater service does not validate what hostname the client was requesting and responds to such requests.
Blizzard DNS Rebinding Attack — Proof of Concept Exploit

Ormandy has also published a proof-of-concept exploit that executes DNS rebinding attack against Blizzard clients and could be modified to allow exploitation using network drives, or setting destination to "downloads" and making the browser install malicious DLLs, data files, etc.
Ormandy responsibly reported Blizzard of the issue in December to get it patched before hackers could take advantage of it to target hundreds of millions of gamers.

However, after initially communication, Blizzard inappropriately stopped responding to Ormandy's emails and silently applied partial mitigation in the client version 5996.
"Blizzard was replying to emails but stopped communicating on December 22nd. Blizzard is no longer replying to any enquiries, and it looks like in version 5996 the Agent now has been silently patched with a bizarre solution," Ormandy says.

"Their solution appears to be to query the client command line, get the 32-bit FNV-1a string hash of the exename and then check if it's in a blacklist. I proposed they whitelist Hostnames, but apparently, that solution was too elegant and simple. I'm not pleased that Blizzard pushed this patch without notifying me, or consulted me on this."

After the Ormandy's report went public, Blizzard contacted and informed him that a more robust Host header whitelist fix to address the issue entirely is currently being developed for deployment.
Ormandy is also checking other big games vendors with a user base of over 100 Million to see if the problem can be replicated.