

[HISPASEC] Blizzard StarCraft Brood War 1.15.1 Remote DoS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-08/msg00451.html>

- *From:* "Gynvael Coldwind" <gynvael@xxxxxxxxxxxxxx>
 - *Date:* Wed, 29 Aug 2007 14:24:30 +0200
-

HISPASEC
Security Advisory
<http://blog.hispasec.com/lab/>

Name : Blizzard StarCraft Brood War Remote DoS
Class : Remote/Local DoS
Threat level : MED
Discovered : 2007-08-08
Published : 2007-08-29
Credit : Gynvael Coldwind
Vulnerable : StarCraft Brood War 1.15.1 and prior
StarCraft 1.15.1 and prior may also be affected

== Abstract ==

StarCraft is a real-time strategy game by Blizzard Entertainment.

StarCraft fails to handle exceptional conditions when generating a minimap preview of a malformed map. Additionally, since StarCraft includes a map distribution mechanism (allowing players that do not own a map to download it when entering a game) it is possible to send a malformed map to a player that enters the game, and so, remotely DoS his application.

== Details ==

When a player enters a StarCraft Brood War game (local, lan game or an Internet Battle.net game) a preview of the map is generated. If the map was malformed StarCraft tries to read an area which is not allocated. This leads to a Denial of Service condition, since StarCraft generates an Access Violation (READ) exception which is not handled.

Additionally, if a player enters a multiplayer game, and he does not own a map that the game is taking place on, StarCraft downloads the map from other players (not just the creator of the game). If StarCraft downloads a malformed map from a remote player, it will try to generate

[HISPASEC] Blizzard StarCraft Brood War 1.15.1 Remote DoS

a minimap and enter the DoS condition (this has been confirmed in testing).

Since StarCraft is a full screen DirectX application a DoS may cause a need to reboot the whole system on older Windows systems.

Proof of Concept map:

http://blog.hispasec.com/lab/files/SC_PoC_DoS.scm

Memory patcher disabling minimap preview generation:

http://blog.hispasec.com/lab/files/SC_Patch.c

http://blog.hispasec.com/lab/files/SC_Patch.exe (compiled binary)

== Vendor status and solution ==

The vendor has been informed but has not yet released a proper patch (a fix for this issue was not included in the 1.15.1 patch).

The solution is to be careful when joining games on unknown maps. See SC_Patch.c and SC_Patch.exe (links in the Details section) for a memory patcher that disables minimap preview generation in the running StarCraft application.

== Disclaimer ==

This document and all the information it contains is provided "as is", without any warranty. Hispasec Sistemas is not responsible for the misuse of the information provided in this advisory. The advisory is provided for educational purposes only.

Permission is hereby granted to redistribute this advisory, providing that no changes are made and that the copyright notices and disclaimers remain intact.

Copyright (C) 2007 Hispasec Sistemas.

—

Gynvael Coldwind

mailto:gynvael@xxxxxxxxxxxxxx

mailto:michael@xxxxxxxxxxxxxx