In-game callvote map buffer-overflow in Call of Duty series

In-game callvote map buffer-overflow in Call of Duty series

2006-09-26 00:12 von Kelli (0 Kommentare)

Luigi hat einen Patch für Call of Duty 1, Call of Duty UO und Call of Duty 2 fertiggestellt der einen Vote Bug in diesen Spielen beseitigt. Durch den Fehler ist es möglich einen Server auf dem die Abstimmung erlaubt ist zu crashen. Luigis Patch ist natürlich nicht Offiziell und sollte nur eingespielt werden wenn der Server konkret unter solchen Attacken leitet. Er wird nicht für Clients benötigt, und man braucht ihn auch nicht wenn das Voten auf dem Server deaktiviert ist.

Der Patch ist für Windows und Linuxserver verfügbar, Mac Server (gibts sowas?) bleiben verwundbar. Details und Patch bei http://aluigi.altervista.org/adv/codmapbof-adv.txt

Update:
Luigi hat auch einen Patch für den info string Überlauf fertiggestellt. Das Problem hierbei: Der Infostring enthällt Pfade, benutzte iwd Dateien, Checksummen für diese Dateien, die Maprotation, den Servernamen u.s.w. Aus irgendeinen Grund ist dieser String mit 1024Byte so knapp bemessen das er regelmäßig überläuft was dann gleich den Server crasht. Luigi kann die Speicherzuordnung nicht ändern, behauptet ja sogar Activision das sie das nicht können**[1]**. Aber er kann die exception abfangen und verhindern das der Server crasht. Dies ist keine Lösung um mehr Maps zum laufen zu bekommen und zur Zeit ist keine Methode bekannt wie man diesen Fehler remote ausnutzen kann. Wer dennoch den Patch installieren möchte, zum Beispiel wenn man selbst Anbieter von CoD(2) Servern ist und verhindern möchte das der "Mieter" dieser Server die regelmäßig crasht. http://aluigi.altervista.org/patches/cod2vawo.lpatch

[1] gute-nachricht-schlechte-nachricht

Zurück