Medal of Honor verwundbar Medal of Honor verwundbar

2006-05-13 05:16 von Kelli (0 Kommentare)

Das allseits bekannte und beliebte Spiel Medal of Honor enthält eine kritische Lücke durch die es möglich ist dem Server Code unterzujubeln (Buffer Overflow) Das besonders traurige daran ist, das es wegen des für Spiele relativ "hohen Alters" (erschienen 2002) vermutlich keinen Patch mehr von EA geben wird. Um dem Server böses zu tun reicht ein einziges manipuliertes UDP Paket an den Query Port des Moh Servers (der query Port muss immer offen sein, ansonsten ist der Server für niemanden sichtbar und für Spieler auch nicht erreichbar) reicht um den Code unterzuschieben.

Luigi Auriemma, der den Fehler fand hat gleich einen eigenen Patch [1] für das Problem veröffentlicht, der jedoch im Moment nur für Windows Server verfügbar ist. Das überaus witzige daran ist, das der Patch nur funktioniert wenn man das Orginal EA Binary gegen sein No-CD Pendant austauscht, da der verwundbare Teil in ebend diesem verschlüsseltem Bereich liegt.

lol -> Orginal: Verwundbar
_pöse_Version: Patch verfügbar.

So ganz nebenbei beseitigt Luigi dann auch gleich überflüssiges "Leergut" im Code mit seinem Patch und macht den Code so etwas schneller. Im Moment kann man Windosen Besitzer nur zu dem Patch raten, und Moh Pinguine am besten abschalten. Das Risiko sich bei dem verwenden einer No-CD Version auf dem Win Server gleich auf direktem Weg ein rootkit einzufangen weil der No-CD Patch auch noch andere Dinge enthält, sollte man aber nicht unterschätzen. Dagegen hilft dann kein Patch und keine Geisterbeschwörung.

[1] Patch Moh Win http://aluigi.altervista.org/patches/mohaaboffix.zip

Zurück