Medal Of Honor Allied Assault Remote Buffer Overflow Vulnerability Medal Of Honor Allied Assault Remote Buffer Overflow Vulnerability

2004-07-21 23:44 von Kelli (0 Kommentare)

In Medal of Honor wurde ein Fehler entdeckt der es erlaubt beliebigen Code einzuschleußen.
Wie auf Securityfocus berichtet wurde, betrifft der Fehler alle Versionen von Medal of Honor einschließlich der diversen Mods und Erweiterungen wie Spearhead, Breaktrouth u.s.w.

Ein "Buffer Overflow" meint, das durch schicken von (un)gültigen bzw überlangen Parametern der für die Anwendung vorgesehene Bereich des Arbeitsspeichers "überflutet" wird.
Dadurch verschiebt sich die Addressierung.Durch geschicktes Ausnutzen dieser Speicherverschiebung kann man Code in den z.B. für das Betriebssystem vorgesehenen Bereich des Arbeitsspeichers bringen, der dann mit diesen Privillegien ausgeführt wird.

Dennoch ist der Fehler in MoH nicht ganz so tragisch da er sich "nur" im LAN Modus ausnutzen lässt. Im Internet Modus wird dieser Teil der Arbeit von Gamespy ersetzt.Und die Personenzahl bei einem LAN Game ist doch eher überschaubar.
Wer seinen LAN Partnern nicht traut, für den gibt es einen Inoffiziellen Patch unter http://www.securityfocus.com/data/vulnerabilities/patches/mohaaboffix.zip

Orginal Meldung auf Securityfocus.com:
A remote buffer overflow vulnerability was reported in Medal of Honor Allied Assault.

This issue may permit remote code execution in vulnerable game servers and clients. However, it is reported that clients will only be affected in LAN games as Internet games use the Gamespy protocol. The issue also affects various expansion packs for the game.

Solution:
Workaround:
An unofficial, third-party patch for Windows versions has been released:

http://www.securityfocus.com/data/vulnerabilities/patches/mohaaboffix.zip

This patch has not been tested by Symantec.

Quelle:
http://www.securityfocus.com/bid/10743/info/

Zurück