

[VulnWatch] LutelWall <= 0.97 insecure temporary file creation

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-06/0003.html>

From: ZATAZ Audits (*exploits_at_zataz.net*)

Date: 06/06/05

Date: Mon, 06 Jun 2005 10:21:54 +0200

To: vulldb@securityfocus.com, vuln@secunia.com, vuln@k-otik.com, moderators@osvdb.org, bugs@securi

#####

LutelWall insecure temporary file creation

Vendor: <http://firewall.lutel.pl/index.php>

Advisory: <http://www.zataz.net/adviso/lutelwall-05222005.txt>

Vendor informed: yes

Exploit available: yes

Impact : medium

Exploitation : low

#####

The vulnerability is caused due to temporary file being created insecurely.

This can be exploited via symlink attacks to create and overwrite arbitrary files

with the privileges of the user running the affected script.

The exploitation require that the root try to update the software.

#####

Versions:

#####

LutelWall <= 0.97

#####

Solution:

#####

non solution yet.

#####

Timeline:

#####

VulnWatch: [VulnWatch] LutelWall <= 0.97 insecure temporary file creation

Discovered : 2005-05-22
Vendor notified : 2005-05-22
Vendor response : none
Vendor fix : no fix
Disclosure : 2005-06-06

Technical details :
#####

Vulnerable code :

```
-----  
  
# Prefix of temporary firewall files  
tmp='/tmp/lutelwall'  
  
new_version_check () { # Check for new version of script  
  
if [ "`wget -V 2>&1 >/dev/null`" ]; then  
    message 3 "Warning: Wget is required to check for updates."  
else  
    new_ver=`wget -C off -O - -q -t 1 -T 3 -w 3 -U "\`uname -a 2>&1\  
http://firewall.lutel.pl/ver`  
    if [ `echo $current_version | gawk '{ gsub("\\\\.", ""); print 1$0 }`  
-lt `echo $new_ver | gawk '{ gsub("\\\\.", ""); print 1$0 }` ]; then  
        echo -e "\nThere is newer version of LutelWall (${new_ver})"  
        echo -n " Changes since previous version:"  
        echo `wget -C off -O $tmp-newfeat -q -t 1 -T 3 -w 3  
http://firewall.lutel.pl/FEATURES-${new_ver}`  
        cat $tmp-newfeat  
        echo "Do you want to update [y/N]? "  
        read -s -t 5 -n 1 ln  
        if [ "$ln" = 'y' -o "$ln" = 'Y' ]; then  
            wget -O $tmp-script -q -T 3 http://firewall.lutel.pl/lutelwall  
            cat $tmp-script > $0  
            rm -rf $tmp-script  
            echo "Your firewall is up to date, exiting after update!"  
            exit  
        else  
            message 5 "Update aborted"  
        fi  
    else  
        message 5 "LutelWall is up-to-date"  
    fi;  
fi;  
  
}
```


Related :
#####

VulnWatch: [VulnWatch] LutelWall <= 0.97 insecure temporary file creation

nothing related

#####

Credits :

#####

Eric Romang (eromang@zataz.net – ZATAZ Audit)