MWR InfoSecurity Security Advisory

Watchguard Firebox PPTP VPN User Enumeration Vulnerability

4th April 2008

MWR INFOSECURITY

MWR INFOSECURITY

CONTENTS

MWR INFOSECURITY

Watchguard Firebox PPTP VPN User Enumeration Vulnerability

Package Name:	Watchguard Firebox
Date:	2008-04-04
Affected Versions:	Firebox software prior to version 10

CVE Reference	CVE-2008-1618
Author	Luke Jennings
Severity	Medium Risk
Local/Remote	Remote
Vulnerability Class	Information Disclosure
Vendor Response	Watchguard have released a patch to address the issue.
Exploit Details Included	Yes
Versions Affected	Firebox software prior to version 10

Timeline:

Vulnerability Reported to vendor	2007-11-05
Vendor Patch Released	2008-02-11
Advisory Released	2008-04-04

Overview:

The PPTP VPN service offered by Watchguard Firebox allows valid usernames to be enumerated.

Impact:

The impact of this vulnerability is that password guessing attacks can be performed much more efficiently by conducting them only against those usernames known to be valid. Additionally, these usernames may be valid on other systems and may also aid social engineering attacks.

Cause:

During the MS-CHAPv2 authentication handshake different error codes are returned depending on whether or not the username supplied is valid.

Interim Workaround:

The vulnerability cannot be used to request valid usernames but only to determine whether a given username is valid. Consequently, ensuring all usernames are difficult to guess will provide some protection against this vulnerability.

Solution:

Watchguard have addressed this issue as of version 10 of their Firebox software: -

https://www.watchguard.com/archive/softwarecenter.asp

Please note these fixes have not been tested by MWR InfoSecurity.

MWR INFOSECURITY

1 Detailed Vulnerability Description

1.1 Introduction

Watchguard Firebox is primarily a firewall based product and is described as follows on the Watchguard website: -

"The Firebox® X family of UTM security appliances delivers the industry's best combination of strong security, reliability, and performance – all at a compelling price point. IT administrators have granular controls to manage the network, with unprecedented visibility into network activity. Continually updated security subscriptions boost protection in critical attack areas to block spam, spyware, web-based exploits, and blended threats for comprehensive defenses. All of this is backed by a team of security professionals who provide the expert guidance and support to keep your security solution in top form."

Source: https://www.watchguard.com/products/

1.2 Technical Background

The Watchguard Firebox can be configured to allow remote user access through the use of the PPTP VPN service. When enabled this can normally be detected remotely through the presence of an open TCP port (1723) and the device's acceptance of the GRE protocol (IP protocol number 47).

The PPTP VPN service uses MS-CHAPv2 for authentication. This relies on a challenge/response mechanism in order to successfully authenticate users. When a remote user attempts to authenticate with the PPTP VPN service, an MS-CHAPv2 packet should be returned indicating success or failure. Failure is indicated by the return of a code 4 MS-CHAPv2 packet. This packet will additionally contain a value in the form "E=<error_number>" which indicates the type of error that occurred. A list of common error codes is given below: -

```
646 ERROR_RESTRICTED_LOGON_HOURS
647 ERROR_ACCT_DISABLED
648 ERROR_PASSWD_EXPIRED
649 ERROR_NO_DIALIN_PERMISSION
691 ERROR_AUTHENTICATION_FAILURE
709 ERROR_CHANGING_PASSWORD
```

The vulnerability occurs as a consequence of differences in the error codes returned in the failure packet which are dependent on whether or not the username supplied is valid. When a valid username is given with an incorrect password the following response is returned: -

```
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x444fc9b9> <accomp>]
rcvd [LCP ConfReq id=0x1 <mru 338> <auth chap MS-v2> <magic 0xfa52b227> <pcomp>
<accomp>]
sent [LCP ConfRej id=0x1 <pcomp>]
rcvd [LCP ConfRej id=0x1 <asyncmap 0x0>]
sent [LCP ConfReq id=0x2 <magic 0x444fc9b9> <accomp>]
rcvd [LCP ConfReq id=0x2 <mru 338> <auth chap MS-v2> <magic 0xfa52b227> <accomp>]
sent [LCP ConfAck id=0x2 <mru 338> <auth chap MS-v2> <magic 0xfa52b227> <accomp>]
rcvd [LCP ConfAck id=0x2 <magic 0x444fc9b9> <accomp>]
sent [LCP EchoReq id=0x0 magic=0x444fc9b9]
rcvd [CHAP Challenge id=0x1 <d15340ea7112ac46f240e4f18fe2a278>, name = "watchguard"]
```

```
sent [CHAP Response id=0x1
<73469ca9bed04ea6f0e5d1be49b47a1a0000000000000000f424ac68e1231f756e1657a2bc25efcd3b7
ba78110bcf48201>, name = "valid_username"]
rcvd [LCP EchoRep id=0x0 magic=0xfa52b227]
rcvd [CHAP Failure id=0x1 "E=691 R=1 Try again"]
MS-CHAP authentication failed: E=691 Authentication failure
CHAP authentication failed
```

However, when an invalid username is supplied, the following response is received: -

```
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x9689f323> <accomp>]
rcvd [LCP ConfReq id=0x1 <mru 338> <auth chap MS-v2> <magic 0x245cdcee> <pcomp>
<accomp>]
sent [LCP ConfRej id=0x1 <pcomp>]
rcvd [LCP ConfRej id=0x1 <asyncmap 0x0>]
sent [LCP ConfReq id=0x2 <magic 0x9689f323> <accomp>]
rcvd [LCP ConfReq id=0x2 <mru 338> <auth chap MS-v2> <magic 0x245cdcee> <accomp>]
sent [LCP ConfAck id=0x2 <mru 338> <auth chap MS-v2> <magic 0x245cdcee> <accomp>]
rcvd [LCP ConfAck id=0x2 <magic 0x9689f323> <accomp>]
sent [LCP EchoReq id=0x0 magic=0x9689f323]
rcvd [CHAP Challenge id=0x1 <d15340ea7112ac46f240e4f18fe2a278>, name = "watchguard"]
sent [CHAP Response id=0x1
<73469ca9bed04ea6f0e5d1be49b47a1a0000000000000000f424ac68e1231f756e1657a2bc25efcd3b7
ba78110bcf48201>, name  = "invalid_username"]
rcvd [LCP EchoRep id=0x0 magic=0x245cdcee]
rcvd [CHAP Failure id=0x1 "E=649 R=1 Try again"]
MS-CHAP authentication failed: E=649 No dialin permission
CHAP authentication failed
```

As can be seen, the error codes differ according to whether a valid or invalid username is supplied. A valid username results in an “E=691 Authentication Failure” error response, whereas an invalid username results in an “E=649 No dialin permission” error response. This difference can be used to discriminate between valid and invalid users.

The ability to determine valid usernames would allow an attacker to conduct password guessing attacks against the PPTP VPN service much more efficiently as they would be able to target only those usernames known to be valid. A compromised account could then be used to access the internal network normally protected by the PPTP VPN service. Additionally, it is common for organisations to use standard username formats across systems. Therefore, usernames determined to be valid may be used to aid an attacker in penetrating other systems. They may also be useful in conducting social engineering attacks, as knowledge of valid usernames may allow an attacker to appear to be more informed than an outsider would be expected to be.

1.3 Exploit Information

The most likely attack vector would be to construct an automated script that could perform dictionary and brute force attacks against the PPTP VPN service in order to determine valid usernames. These could then be utilised for further attacks by performing automated password guessing attacks against these valid usernames or using them to aid social engineering attacks.

The speed at which this could be performed would be dependent on the bandwidth between the attacker and the target system and any inbuilt protection to reduce brute force attacks by limiting the number of connections within a given time frame.

1.4 Dependencies

The impact of this vulnerability would be dependent upon:

- the number of valid VPN users
- whether the usernames were easily guessable
- the strength of the password policy
- the extent of internal network access permitted by the VPN
- the number of other systems for which the usernames were also valid

2 References

The following RFCs provide more information about the CHAP and MS-CHAPv2 protocols: -

http://www.faqs.org/rfcs/rfc1994.html
http://www.ietf.org/rfc/rfc2759.txt

The following is a link to the patches released by Watchguard: -

https://www.watchguard.com/archive/softwarecenter.asp

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