



CSIS Security Research and Intelligence

Advisory - BlueCoat K9 Web Protection 3.2.36 Overflow

VU#271601

CVE-2007-1685

Discovered by Dennis Rand
rand@csis.dk
<http://www.csis.dk>

CSIS Security Group

A. P. Møllers Alle 11 • DK-2791 Dragør • Tlf. +45 8813 6030 • Fax +45 2817 6030
info@csis.dk • www.csis.dk • CVR 29523355

Table of contents

Table of contents	2
Introduction	3
Timeline of public disclosure	3
Contact information	3
PGP Public Key	4
File description.....	5
Installation file	5
Service file	5
Technical details	6
Abstract	6
Description	6
Analysis	8
Detection	8
Recovery	9
Exploit	10
Proof of concept 1.....	10
Proof of concept 2.....	10
Workaround.....	11
Fix.....	11
What are CVSS	12
Disclaimer	13

Introduction

The installation has been made on a clean new installed Windows 2000 Server with Service Pack 4 running with the latest patch level.

A free version of the product can be downloaded from **<http://www.k9webprotection.com>**

Severity rating: High Risk

CVSS Vector: (AV:R/AC:L/Au:NR/C:C/I:C/A:P/B:N)

Timeline of public disclosure

- 14-03-2007 Vulnerability discovered.
- 27-03-2007 Research ended.
- 01-04-2007 CERT/CC informed
- 02-04-2007 Received CERT/CC tag VU#271601
- 02-04-2007 Vendor contacted to get a contact person
- 04-04-2007 Sent report to Ross, Jonathon [jonathon.ross@bluecoat.com]
- 04-04-2007 Received CVE tag from CERT/CC - CVE-2007-1685
- 11-04-2007 Response from (Lakhani, Joe [joe.lakhani@bluecoat.com])
- 08-05-2007 Verified patch from BlueCoat.
- 04-06-2007 BlueCoat released patched version (3.2.44)
- 05-06-2007 Released information to CSIS Platinum list
- 07-06-2007 Public release

Contact information

The following vulnerability were discovered by Dennis Rand at CSIS.DK
Questions regarding this issue should be directed to:

Dennis Rand
rand@csis.dk

File description

Installation file

File name: k9-webprotection.exe
Company Name: Blue Coat Systems, Inc.
MD5 Check Sum: a030de5b943d714546001b4383c23d64
SHA-1 Check Sum: c6c92a24db8e4ac44e33f8b8cc68e299fcf45506

Service file

File name: k9filter.exe
Company Name: Blue Coat Systems, Inc.
Program version: 3.2.36
Filter version: 3.2.32
Service license: K9-00004
MD5 Checksum: 2cc4d03e587b5d7fe99a23b3c48023f9
SHA-1 Checksum: 62784624195644ba1a198a0118ca990aee4c93ee
Default path: C:\Program Files\Blue Coat K9 Web Protection\k9filter.exe

Technical details

Abstract

We have discovered a remote exploitable arbitrary overwrite flaw, in the Blue Coat K9 Web Protection local Web configuration manager on 127.0.0.1 and port 2372. This allows an attacker to perform at least a Denial of Service condition, on the usage of internet.

Since the overflow results in an overwrite of the return address remote code execution is possible.

The attack vector could also be privilege escalation on the local machine.

Description

Remote exploitation of an arbitrary overwrite, in the Blue Coat K9 Web Protection local Web configuration manager on 127.0.0.1 and port 2372.

This allows an attacker to perform at least a Denial of Service condition, on the usage of internet.

Since the overflow results in a overwrite of the return address remote code execution is possible.

The attack vector could also be privilege escalation.

The services are as default running with system privileges.

The flaw seems to be due to an unchecked buffer allowing filling up the buffer where the address that the SEH are pointing to are controlled by the attacker.

Last few steps before full control:

77FBB24F	FF75 0C	PUSH DWORD PTR SS:[EBP+C]
77FBB252	52	PUSH EDX
77FBB253	64:FF35 00000000	PUSH DWORD PTR FS:[0]
77FBB25A	64:8925 00000000	MOV DWORD PTR FS:[0],ESP
77FBB261	FF75 14	PUSH DWORD PTR SS:[EBP+14]
77FBB264	FF75 10	PUSH DWORD PTR SS:[EBP+10]
77FBB267	FF75 0C	PUSH DWORD PTR SS:[EBP+C]
77FBB26A	FF75 08	PUSH DWORD PTR SS:[EBP+8]
77FBB26D	8B4D 18	MOV ECX,DWORD PTR SS:[EBP+18]
77FBB270	FFD1	CALL ECX

When sending a special crafted HTTP GET request to 127.0.0.1 on port 2372:

Proof of Concept:
 http://127.0.0.1:2372/home.html<Ax168><DCBA><A x 56><BBBB><AAAA>

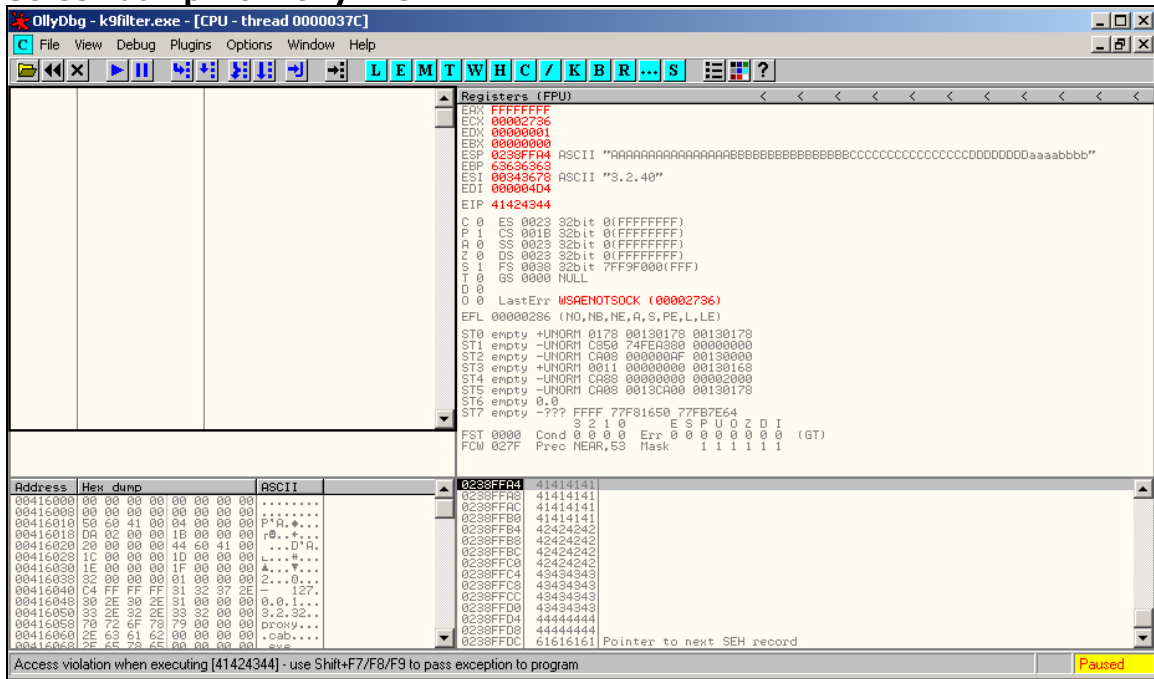
Return Address = DCBA
 Pointer to the next SEH record = BBBB
 SE Handler = AAAA

Good breakpoints in OllyDBG when analyzing the vulnerability

Call recv

```
.text:004144BC ; int __stdcall recv(SOCKET s,char *buf,int len,int flags)
.text:004144BC recv
sub_412A7E+66
.text:004144BC jmp ds:__imp_recv
.text:004144BC recv
endp
```

Screen dump from OllyDBG



Analysis

Exploitation of this vulnerability would result in at least a Denial of Service condition against the user.

But the main usage would be remote code execution when getting the user of BlueCoat K9 to visit a malicious page or a person who wants to locally escalate his or her privileges.

Detection

We have confirmed the existence of this problem in Blue Coat K9 Web Protection 3.2.36. It is suspected that earlier versions are also affected.

Recovery

At manual restart of the service is a requirement, after an attack has been preformed.

The user will notice the problem due to the following error page whenever they try to visit a page



The screenshot shows a web browser window with the address bar displaying `http://www.csis.dk/`. The main content area features a header with a dog icon and the text "K9 Web Protection Alert". Below this is a dark blue bar with a red warning icon and the text "K9 Error". The main body of the page contains a red warning icon followed by the heading "K9 Web Protection Not Responding". The text below explains that the Blue Coat K9 Web Protection program is not responding, preventing the requested web page from being displayed. It lists three potential causes: temporary unavailability, a crash, or a corrupted installation, each with a proposed solution. A link is provided for further support options.

Address  `http://www.csis.dk/`

 **K9 Web Protection Alert**

 **K9 Error**

 **K9 Web Protection Not Responding**

The Blue Coat K9 Web Protection program is not responding.

The Web page you requested could not be displayed, because the K9 Web Protection program is not responding.

There are many different reasons why this could be happening. Please try the following:

- **K9 Web Protection was temporarily unavailable**
Proposed Solution: Refresh this page to try again.
- **K9 Web Protection has crashed**
Proposed Solution: Reboot your computer so K9 Web Protection can start again.
- **Your K9 Web Protection installation has become corrupted**
Proposed Solution: Reinstall K9 Web Protection. NOTE: You may be asked for your license key and/or administrative password to reinstall.

If this problem persists, please [click here](#) to view other support options.

Workaround

We are currently not aware of any workaround for the vulnerability.

Fix

A patch has been released by BlueCoat, applying version 3.2.44 or higher will fix the problem.

What are CVSS

The National Infrastructure Advisory Council (NIAC) has chosen FIRST to be the custodian of the Common Vulnerability Scoring System (CVSS), the emerging standard in vulnerability scoring. This rating system is designed to provide open and universally standard severity ratings of software vulnerabilities. There is a critical need to help organizations appropriately prioritize security vulnerabilities across their constituency. The lack of a common scoring system has security teams worldwide solving the same problems with little or no coordination. FIRST will closely collaborate with CERT/CC and MITRE on this.

<http://www.first.org/cvss/>

Disclaimer

The information within this document may change without notice.
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages,
including direct, indirect, incidental, consequential, loss of business profits or special
damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and
unregistered trademarks represented in this document
is the sole property of their respective owners.

If you use the following information you have to credit CSIS Security Group and the
Researcher for the discovery.