**ASP.NET Padding Oracle Vulnerability**

### Issue
ASP.NET uses encryption to hide sensitive data and protect it from being tampered by the client. However, a vulnerability in the ASP.NET encryption implementation could allow an attacker to decrypt and tamper with this data. This vulnerability exists in all versions of ASP.NET.

### IMPACT:
An attacker who exploits this vulnerability could view data, such as the View State, which was encrypted by the target server, or read data from files on the target server, such as web.config, and could tamper with the contents of the data. By sending back the altered contents to an affected server, the attacker could observe the error codes returned by the server.

### Applies to

<table>
<thead>
<tr>
<th>SecureAuth IdP Version</th>
<th>OS Version</th>
<th>Background Information</th>
</tr>
</thead>
</table>
| 6.x+ (see Disclaimer)  | • Windows Server 2008  
                        | • Windows Server 2008 R2 | According to Microsoft Security Bulletin MS10-070 this vulnerability was  
|                        |                    | • introduced in 2010 in Microsoft .NET Framework 3.5 Service Pack 1  
|                        |                    | • resolved after Microsoft .NET Framework version 4.0 |

### Disclaimer
SecureAuth applies the latest Microsoft security updates on all SecureAuth IdP appliances before shipment.

**NOTE:** Any SecureAuth IdP appliance out in the field before the occurrence of this vulnerability may be affected if the security update referenced in this article has not yet been applied at the user's site.

This note also pertains to SecureAuth IdP appliances out in the field that have been upgraded to the latest SecureAuth IdP software release version at the user's site.
**Recommendation**

1. Apply the Microsoft patch MS10-070 linked in the Web references section

2. Implement this configuration change to all web.config files on ALL realms on ALL SecureAuth IdP appliances, if it not already implemented

**Vulnerable code**

```xml
<customErrors defaultRedirect="customerror.htm" mode="On" />
```

**More Secure Updated code**

```xml
<customErrors redirectMode="ResponseRewrite" defaultRedirect="customerror.htm" mode="On" />
```

**References**

- Vulnerability in ASP.NET Could Allow Information Disclosure (MS10-070)
- How to check if your application is vulnerable to the ASP.NET Padding Oracle Vulnerability
- Vulnerability in ASP.NET Could Allow Information Disclosure
- Important: ASP.NET Security Vulnerability
- Understanding the ASP.NET Vulnerability