

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

September 29, 2010

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2010-070

DATE(S) ISSUED:

9/29/2010

SUBJECT:

Vulnerability in ASP.NET Could Allow for Information Disclosure

OVERVIEW:

A vulnerability was discovered in Microsoft ASP.NET <<http://ASP.NET>> on September 17, 2010 which could allow for remote information disclosure. ASP.NET <<http://ASP.NET>> allows developers to build dynamic Web applications and Web services. Successful exploitation of this issue may allow an attacker to decrypt sensitive data encrypted by the ASP.NET <<http://ASP.NET>> server or read data from arbitrary files within an ASP.NET <<http://ASP.NET>> application.

Microsoft has reported that the vulnerability is being actively exploited at this time.

SYSTEMS AFFECTED:

- Microsoft .NET Framework 4.0 and earlier
- Microsoft SharePoint Services
- Microsoft SharePoint Server 2010

- Microsoft SharePoint Server 2007

RISK:

Government:

- Large and medium government entities: High
- Small government entities: High

Businesses:

- Large and medium business entities: High
- Small business entities: High

Home users: High

DESCRIPTION:

A vulnerability was discovered in Microsoft ASP.NET <http://ASP.NET> on September 17, 2010 which could allow for remote information disclosure. Specifically, an attacker can retrieve cipher text from the vulnerable ASP.NET <http://ASP.NET> server by viewing the HTML source of the page. The attacker can then send this cipher text via a web request to the server which will reply back with an error message. By analyzing the error message sent by the server, the attacker can determine if the cipher text was decrypted properly or not. If the attacker repeats this process they may be able to gain enough information on how to decrypt the cipher text encrypted by the server. This attack is known as a 'padding oracle' attack. The term 'oracle' refers to a cryptographic system which is used to determine whether a test has passed or failed.

ASP.NET <http://ASP.NET> encrypts sensitive information such as cookie data using a hidden field called '__VIEWSTATE' before sending data to the client. Successful exploitation of this issue may allow an attacker to decrypt sensitive data encrypted by the ASP.NET <http://ASP.NET> server or read data from arbitrary files within an ASP.NET <http://ASP.NET> application. This could lead to an attacker being able to encrypt data in the same fashion as the ASP.NET <http://ASP.NET> server, which would allow them to create their own valid super user cookies. If the attacker passes this super user cookie to the server, the server will accept the cookie and grant the attacker super user privileges in the context of the vulnerable web application. Depending on the privileges associated with the super user of the web application, an attacker could then install programs; view,

change, or delete data; or create new accounts with full user rights.

Microsoft has reported that the vulnerability is being actively exploited at this time.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Consider implementing the follow workarounds suggested by Microsoft
- Enable a UriScan or Request Filtering rule.
- Enable ASP.NET <http://ASP.NET> custom errors.
- Map all error codes to the same error page.
- Consider adding a random sleep delay to the error page.
- Consider blocking requests that modify ASP.Net <http://ASP.Net> application error path on the request querystring.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS10-070.mspx>

Secunia:

<http://secunia.com/advisories/41409/>

Security Focus:

<http://www.securityfocus.com/bid/43316>

TrendMicro:

<http://threatinfo.trendmicro.com/vinfo/secadvisories/default6.asp?VName=Vulnerability+in+ASP.NET+Could+Allow+Information+Disclosure+%282416728%29>

SANS Diary:

<http://isc.sans.edu/diary.html?storyid=9625>

ScottGu's Blog:

<http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-security-vulnerability.aspx>