

**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

July 11, 2007

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.

STATE OF ALASKA ADVISORY NUMBER:

2007-019

DATE ISSUED:

7/11/2007

SUBJECT:

Vulnerabilities in Microsoft .NET Framework Could Allow Remote Code Execution

OVERVIEW:

Microsoft has released Security Bulletin (MS07-040), which identifies three vulnerabilities in the Microsoft .NET Framework. The .NET Framework is Microsoft's managed code programming model for applications. ASP.NET is a part of Microsoft's .NET framework that is used to build web sites and web applications. Two of the vulnerabilities allow a successful attacker to execute malicious code on the system. These vulnerabilities can be exploited by a user visiting a malicious website.

The third vulnerability affects web servers running ASP.NET and, if exploited, can result in information disclosure. An attacker may exploit this vulnerability by sending a specially crafted URL request to the web server. This may allow the attacker to gain access to sensitive information included in configuration files (such as usernames and passwords).

SYSTEMS AFFECTED:

- Microsoft .NET Framework 1.0
- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 2.0

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: **Medium**

DESCRIPTION:

MS07-040 details three new vulnerabilities; two affect systems with the .NET framework installed (.NET PE Loader & .NET JIT Compiler) while the third targets web servers running ASP.NET. The .NET PE Loader vulnerability requires extensive user interaction in order to be successfully exploited. Exploitation of this vulnerability occurs if a user visits a web site, opens an email attachment, or accesses other media that contains malicious content and then performs several other actions to open the file. The .NET JIT Compiler vulnerability requires the user access a specially-crafted file, and could be exploited if a user visits a malicious web site, opens an email attachment, or accesses other media that contains malicious content. Successful exploitation could lead to the execution of arbitrary code. The code would be executed with the privileges of the current user.

The vulnerability affecting ASP.NET can allow an attacker to bypass ASP.NET security validation, which may lead to information disclosure. ASP.NET stores application and web server settings in XML format (e.g. 'web.config' and 'machine.config'). A user attempting to access these files on a web server should receive a '403 Forbidden' error message. By crafting a specially designed URL request, an attacker can potentially bypass this security to view the configuration files.

Examples of the configuration files can be seen at the following sites:

[http://msdn2.microsoft.com/En-US/library/ackhksh7\(VS.71\).aspx](http://msdn2.microsoft.com/En-US/library/ackhksh7(VS.71).aspx)

<http://www.csharpfriends.com/Articles/getArticle.aspx?articleID=106>

An example of the malformed URL request may look similar to:

[http://www.example.tld/\[path\]/somescript.asp%00](http://www.example.tld/[path]/somescript.asp%00)

As can be seen, the ASP.NET developer can make use of the web.config file to store any information necessary for use by the application. Examples of this can be database connection credentials, public/private key data, system usernames, and passwords. The primary concern is not the initial information disclosure this vulnerability allows, but rather the secondary attacks that may be launched using the information gathered.

RECOMMENDATIONS:

We recommend that the following actions be taken:

- Apply all the appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing:
<http://www.microsoft.com/technet/security/bulletin/ms07-040.msp>
- Do not visit unknown or un-trusted Web sites or follow links provided by unknown or un-trusted sources.
- Follow secure programming practices when designing web-based applications.
- Do not store usernames, passwords, or other sensitive information in clear-text form.
- Validate all input before processing data.
- Run applications with least privilege.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS07-040.msp>

<http://support.microsoft.com/kb/931212>

SecurityFocus:

<http://www.securityfocus.com/bid/24778>

<http://www.securityfocus.com/bid/24811>

<http://www.securityfocus.com/bid/24791>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0041>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0042>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0043>