

[NT] ASP.NET Path Validation Vulnerability (MS05-004)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0028.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/09/05

To: list@securiteam.com

Date: 9 Feb 2005 18:27:17 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

ASP.NET Path Validation Vulnerability (MS05-004)

SUMMARY

A canonicalization vulnerability exists in ASP.NET that could allow an attacker to bypass the security of an ASP.NET Web site and gain unauthorized access. An attacker who successfully exploited this vulnerability could take a variety of actions, depending on the specific contents of the website.

DETAILS

Affected Software:

Microsoft .NET Framework 1.0:

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4E6D56E5-3D8D-423B-99A1-41EDF23D65BC>>

Download the update for .NET Framework 1.0 Service Pack 3 for the following operating system versions:

Windows 2000 Service Pack 3 or Service Pack 4

Windows XP Service Pack 1 or Windows XP Service Pack 2,

Windows Server 2003

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=EE611D27-52CF-43DB-BB97-21318C7FAA70>>

Download the update for .NET Framework 1.0 Service Pack 3 for the following operating system versions:

Securiteam: [NT] ASP.NET Path Validation Vulnerability (MS05-004)

Windows XP Tablet PC Edition
Windows XP Media Center Edition

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3271ACD5-EE3C-4BDF-AE28-56D2DF77151E>>

Download the update for .NET Framework 1.0 Service Pack 2 for the following operating system versions:

Windows 2000 Service Pack 3 or Service Pack 4
Windows XP Service Pack 1 or Windows XP Service Pack 2,
Windows Server 2003

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=33D4D33E-473F-4842-A3A8-C8266AEE8FAB>>

Download the update for .NET Framework 1.0 Service Pack 2 for the following operating system versions:

Windows XP Tablet PC Edition
Windows XP Media Center Edition

Microsoft .NET Framework 1.1:

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8EC6FB8A-29EB-49CF-9DBC-1A0DC2273FF9>>

Download the update for .NET Framework 1.1 Service Pack 1 for the following operating system versions:

Windows 2000 Service Pack 3 or Service Pack 4
Windows XP Service Pack 1 or Windows XP Service Pack 2,
Windows XP Tablet PC Edition
Windows XP Media Center Edition

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9BBD5617-49AE-40BF-B0FA-F9049349C6F5>>

Download the update for .NET Framework 1.1 Service Pack 1 for the following operating system versions:

Windows Server 2003

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C5E19719-000F-456A-BEAB-5BD7949F8AA2>>

Download the update for .NET Framework 1.1 for the following operating system versions:

Windows 2000 Service Pack 3 or Service Pack 4
Windows XP Service Pack 1 or Windows XP Service Pack 2,
Windows XP Tablet PC Edition
Windows XP Media Center Edition

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E54BE8BE-22AF-4390-86E1-25D76794D5C7>>

Download the update for .NET Framework 1.1 for the following operating system versions:

Windows Server 2003

CVE Information:

Path Validation Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0847>>

CAN-2004-0847

Mitigating Factors:

Vulnerability only affects sites that require authenticated access.

Workarounds:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified below.

Securiteam: [NT] ASP.NET Path Validation Vulnerability (MS05-004)

* Apply the mitigation code module discussed in Microsoft Knowledge Base article <<http://support.microsoft.com/kb/887289>> 887289. The mitigation code module provides protection on a server-basis.

* An alternative to installing the module on a per application-basis is to make the following change to the global.asax file in the application root directory for each application on an affected system:

```
<script runat=server language=cs>void Application_BeginRequest(object src,
EventArgs e) { if (Request.Path.IndexOf("\\") >= 0 ||
System.IO.Path.GetFullPath(Request.PhysicalPath) != Request.PhysicalPath)
{ throw new HttpException(404, "not found"); }}</script>
```

* Install and Use URLScan. URLScan will help protect against a large number of issues stemming from improperly formed URL requests including the publicly described issues addressed by this bulletin. URLScan does not protect your system as comprehensively as either the mitigation code module or the global.asax script below. Information on URLScan is available here

<<http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp>>
<http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp>.

Frequently Asked Questions:

What is the scope of the vulnerability?

This is an information disclosure vulnerability that could lead to an elevation privilege in some cases. An attacker who successfully exploited this vulnerability could bypass the security of an ASP.NET Web site and gain unauthorized access. An attacker who successfully exploited this vulnerability could take a variety of actions, depending on the specific contents of the Web site.

What causes the vulnerability?

The canonicalization routine that is used by ASP.NET to map the request does not correctly parse the URL.

What is ASP.NET?

ASP.NET is collection of technologies within the .NET Framework that enable developers to build Web applications and XML Web Services.

Unlike traditional Web pages, which use a combination of static HTML and scripting, ASP.NET uses compiled, event-driven pages. This enables developers to build Web-based applications with the same richness and functionality usually associated with applications built in languages such as Visual Basic or Visual C++. Unlike desktop applications, however, these compiled pages generate information that is sent to client desktops or browsers using markup languages such as HTML and XML. This enables developers to build applications with broad functionality, yet project a user interface to devices and systems running many operating systems. Because ASP.NET is a Web-based application environment, it requires an underlying Web server to provide basic HTTP functionality. For this reason, ASP.NET runs on top of IIS 5.0 on Windows 2000, IIS 5.1 on Windows XP and IIS 6.0 on Windows Server 2003.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could gain

Securiteam: [NT] ASP.NET Path Validation Vulnerability (MS05-004)

unauthorized access to parts of a Web site. The actions the attacker could take would depend on the specific content being protected.

Who could exploit the vulnerability?

Any anonymous user who could deliver a specially crafted URL to the affected system could attempt to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by creating a specially crafted URL and sending the URL to an affected system, which could then allow the attacker to bypass the Web site's security.

What systems are primarily at risk from the vulnerability?

Internet-facing systems are primarily at risk from this vulnerability. In addition, internal Web sites that use ASP.NET to host sensitive data can be at risk from this vulnerability.

Could the vulnerability be exploited over the Internet?

Yes. An attacker may be able to exploit this vulnerability over the Internet.

I have already applied the ASP.NET ValidatePath Module (887290) listed in the workarounds section of the bulletin. Do I still need to apply this Security Update?

Yes. While the mitigation is effective, it is still important to apply the security update which removes the vulnerability.

Do I need to uninstall the ASP.NET ValidatePath Module (887290) before applying this update?

No. The module and security update can exist on a system at the same time, although this security update provides all of the benefits that the module does, so it is safe to remove the module once the update is installed.

What does the update do?

The update removes the vulnerability by modifying the way that ASP.NET validates url paths.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number [CAN-2004-0847](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0847).

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

Yes. When the security bulletin was released, Microsoft had received information that this vulnerability was being exploited.

ADDITIONAL INFORMATION

Securiteam: [NT] ASP.NET Path Validation Vulnerability (MS05-004)

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS05-004.msp>>

<http://www.microsoft.com/technet/security/bulletin/MS05-004.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.