

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

9/1/2009

SUBJECT:

Vulnerability in Microsoft IIS Could Lead to Remote Code Execution

OVERVIEW:

A remote buffer overflow vulnerability has been discovered in Microsoft Internet Information Services (IIS) when using the File Transfer Protocol (FTP) server component. IIS is a set of Internet-based services running on Microsoft Windows servers. Successful exploitation could result in an attacker gaining the same privileges as the FTP service. Depending on the privileges associated, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is no patch available for this vulnerability and exploit code is available to the public.

SYSTEMS AFFECTED:

- Microsoft IIS 5.0
 - Microsoft Windows 2000 Advanced Server
 - Microsoft Windows 2000 Advanced Server SP1
 - Microsoft Windows 2000 Advanced Server SP2
 - Microsoft Windows 2000 Datacenter Server SP1
 - Microsoft Windows 2000 Datacenter Server SP2
 - Microsoft Windows 2000 Professional
 - Microsoft Windows 2000 Professional SP1
 - Microsoft Windows 2000 Professional SP2
 - Microsoft Windows 2000 Server
 - Microsoft Windows 2000 Server SP1
 - Microsoft Windows 2000 Server SP2
 - Microsoft IIS 6.0
 - Microsoft Windows Server 2003 Datacenter Edition
 - Microsoft Windows Server 2003 Datacenter Edition Itanium
 - Microsoft Windows Server 2003 Enterprise Edition
 - Microsoft Windows Server 2003 Enterprise Edition Itanium
 - Microsoft Windows Server 2003 Standard Edition
 - Microsoft Windows Server 2003 Web Edition

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: N/A

DESCRIPTION:

A vulnerability has been discovered in Microsoft IIS which could allow an attacker to take complete control of an affected system. This vulnerability is a result of the application failing to perform adequate boundary checks on user-supplied data. More specifically, the vulnerability occurs when handling specially crafted input to the application's FTP server from a malicious user. To exploit this vulnerability, the malicious user must have write privileges to the FTP server; this includes servers that have write access enabled for 'Anonymous' users. At this time, remote code execution is only possible on servers running Microsoft IIS 5.0. Failed exploitation attempts on IIS 5.0 or attacks on IIS 6.0 would result in a Denial of Service (DoS) condition. Successful exploitation could result in an attacker gaining the same privileges as the application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is no patch available for this vulnerability and exploit code is available to the public.

RECOMMENDATIONS:

The following actions should be taken:

Install the appropriate vendor patch as soon as it becomes available after appropriate testing. Unless there is a business need to do otherwise, consider removing write access to FTP server user accounts.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/36189>

Secunia:

<http://secunia.com/advisories/36443>

US-CERT:

<http://www.kb.cert.org/vuls/id/276653>