

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:

3/8/2010

SUBJECT:

Multiple Security Vulnerabilities found in Apache HTTP Server Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Apache Software Foundation's Apache HTTP Server. Apache HTTP Server is one of the most widely used web servers. Successful exploitation of one of these vulnerabilities could result in an attacker gaining SYSTEM-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts. Failed attacks may result in denial-of-service conditions.

SYSTEMS AFFECTED:

Apache Software Foundation Apache 2.2.14 and prior

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:

Multiple vulnerabilities have been discovered in the Apache Software Foundation's Apache HTTP Server. Attackers can leverage these vulnerabilities to execute arbitrary code with SYSTEM-level privileges, gain access to sensitive information or cause a denial-of-service conditions.

'mod_isapi' Module Unload Flaw

A flaw exists within mod_isapi, which would attempt to unload the ISAPI.dll when it encountered various error states. This could leave the callbacks in an undefined state and result in a segfault. On Windows platforms using mod_isapi, a remote attacker could send a specially crafted HTTP requests to trigger this issue. As win32 MPM runs only one process, this condition

would result in a denial-of-service and may be exploited to execute arbitrary code with SYSTEM-level privileges.

Subrequest Handling of Request Headers (mod_headers)

A flaw exists within the core subrequest process code to always provide a shallow copy of the headers_in array to the subrequest. Therefore all modules, such as 'mod_headers', which may manipulate the input headers for a subrequest, would poison the parent request. This can be done one of two ways. Either by modifying the parent request, which might not be intended, or by leaving pointers to modified header fields in memory allocated to the subrequest scope, which could be freed before the main request processing was finished. Thus resulting in a segfault or in revealing data from another request on threaded servers, such as the worker or winnt MPMs.

'mod_proxy_ajp' Denial of Service

A flaw exists within 'mod_proxy_ajp' that would return the wrong status code if it encountered an error. This would also cause a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in denial-of-service.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to Apache 2.2.15 immediately after appropriate testing.

REFERENCES:

Apache Foundation:

http://httpd.apache.org/security/vulnerabilities_22.html

<http://svn.apache.org/viewvc?view=revision&revision=917875>

<http://svn.apache.org/viewvc?view=revision&revision=917870>

https://issues.apache.org/bugzilla/show_bug.cgi?id=48359

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0425>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0434>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0408>

Secunia:

<http://secunia.com/advisories/38776>

Vupen:

<http://www.vupen.com/english/advisories/2010/0511>

Security Focus:

<http://www.securityfocus.com/bid/38494>