

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:

09/17/2012

09/18/2012 – *UPDATED*

09/21/2012 - *UPDATED*

SUBJECT:

Vulnerability in Internet Explorer Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of the vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

~~It should be noted that there is currently no patch available for this vulnerability and~~ **it is currently being exploited in the wild resulting in remote code execution. In addition, the exploit code is currently available as a Metasploit module.**

*September 18 **UPDATED OVERVIEW***

Microsoft has released a workaround for this vulnerability in Security Advisory 2757760.

September 21 **UPDATED OVERVIEW**

Microsoft has released a cumulative update for Internet Explorer that fixes this vulnerability (execCommand Use After Free Vulnerability - CVE-2012-4969) as well as four additional vulnerabilities in an out-of-cycle bulletin MS12-063