

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:

10/08/2013

10/11/2013 - **Updated**

SUBJECT:

Cumulative Security Update for Internet Explorer (MS13-080)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities 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.

October 11 – UPDATED OVERVIEW:

Microsoft has updated security bulletin MS13-080 to remove CVE-2013-3871 from the vulnerabilities addressed by this update. CVE-2013-3871 is scheduled to be addressed in a future security update. Customers who have already successfully updated their systems do not need to take any action.

SYSTEM AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

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: High

DESCRIPTION:

~~Ten~~**Nine** memory corruption vulnerabilities have been discovered in Internet Explorer. These vulnerabilities occur due to the way Internet Explorer improperly accesses objects in memory and could be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerabilities.

Successful exploitation 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.

October 11 – UPDATED DESCRIPTION:

Microsoft has updated security bulletin MS13-080 to remove CVE-2013-3871 from the vulnerabilities addressed by this update. CVE-2013-3871 is scheduled to be addressed in a future security update. Customers who have already successfully updated their systems do not need to take any action.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/security/bulletin/ms13-080>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3871>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3872>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3873>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3874>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3875>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3882>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3885>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3886>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3893>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3897>