

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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE ISSUED:

08/19/2015

SUBJECT:

Vulnerability in Microsoft Internet Explorer Could Allow Remote Code Execution (MS15-093)

OVERVIEW:

A vulnerability has been discovered in Microsoft's web browser, Internet Explorer. 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. A failed attempt at exploiting this vulnerability could cause a denial of service condition.

THREAT INTELLIGENCE:

There are reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- 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

TECHNICAL SUMMARY:

Microsoft Internet Explorer is prone to a memory corruption vulnerability, which could allow for remote code execution. The vulnerability exists when Internet Explorer improperly accesses objects in memory.

This vulnerability could allow an attacker to execute remote code by convincing a victim to visit a specially-crafted website. When the website is visited, the attacker's script will run with the same permissions as the affected user account. 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. A failed attempt at exploiting this vulnerability could cause a denial of service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Apply updates from Microsoft, immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms15-093.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2502>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>