

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:

02/14/2014

02/20/2014 - **Updated**

SUBJECT:

Zero Day Vulnerability in Internet Explorer Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

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. 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.

THREAT INTELLIGENCE:

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild. Microsoft is reporting targeted attacks that attempt to exploit this vulnerability in Internet Explorer 9 and Internet Explorer 10. Multiple vendors are reporting that various compromised sites are serving this zero-day exploit up. It is believed the actors behind this campaign are associated with two previously identified campaigns (Operation DeputyDog and Operation Ephemeral Hydra).

February 20, 2014 UPDATED THREAT INTELLIGENCE:

Microsoft has confirmed that Internet Explorer 6, 7, 8, and 11 are not affected by this vulnerability. Microsoft has released a "Fix It" solution that will apply the workarounds in security advisory 2934088.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10

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:

A vulnerability has been reported that affects all versions 9 and 10 of Internet Explorer that could allow for remote code execution. This vulnerability exists due to the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code, in the context of the current user, within Internet Explorer. An attacker could host a specially crafted website designed to take advantage of this vulnerability, and then convince or trick an unsuspecting user to visit their site.

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.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild. Microsoft is reporting targeted attacks that attempt to exploit this vulnerability in Internet Explorer 9 and Internet Explorer 10.

It has been reported that Internet Explorer 11 is not affected by this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- We recommend the following actions be taken:
- Consider using an alternate browser until a patch is made available for the vulnerable versions of Internet Explorer.
- Upgrade to Internet Explorer 11 after appropriate testing, until a security update has been released that fixes this issue.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

February 20, 2014 UPDATED RECOMMENDATIONS:

- ***Consider implementing the “Fix It” solution provided by Microsoft.***

REFERENCES:

Fireeye:

<http://www.fireeye.com/blog/uncategorized/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html>

Websense:

<http://community.websense.com/blogs/securitylabs/archive/2014/02/14/msie-0-day-exploit-cve-2014-0322-possibly-targeting-french-aerospace-organization.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0322>

SecurityFocus:

<http://www.securityfocus.com/bid/65551>

February 20, 2014 UPDATED REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/advisory/2934088>

<http://blogs.technet.com/b/msrc/archive/2014/02/19/microsoft-releases-security-advisory-2934088.aspx>